FACULTY

ERIC ALDEN, B.A., M.A., J.D.
Assistant Professor of Law
RICHARD A. BALES, B.A., J.D.
Professor of Law & Associate Dean of Faculty Development
DONNA S. BENNETT, A.B., M.A., M.S.L.S.
Professor of Library Services & Assistant Director for User Services
JOHN M. BICKERS, A.B., J.D., LL.M.
Assistant Professor of Law
ROGER D. BILLINGS, JR., A.B., J.D.
Professor of Law
SHARLENE BOLTZ, B.A., J.D.
Professor of Law
CAROL BREDEMEYER, A.B., M.S.L.S.
Professor of Law Library Services & Assistant Director of Faculty Services
ANTHONY E. CHAVEZ, B.S., J.D.
Assistant Professor of Law
URSULA DOYLE, B.A., M.A., J.D.
Assistant Professor of Law
NANCY L. FIRAK B.S., J.D., LL.M.
Professor of Law
CAROL FURNISH, B.A., M.L.S.
Professor of Library Services & Assistant Director for Instruction & Outreach
JON M. GARON, B.A., J.D.
Director of Law and Informatics Institute & Professor of Law
RICHARD GRAVES, B.A., J.D., LL.M., LL.M.
Assistant Professor of Legal Writing
CHRISTOPHER GULINELLO, B.A., J.D., LL.M.
Professor of Law
JACK HARRISON, B.A., J.D.
Assistant Professor of Law
AMY HALBROOK, B.A., J.D.
Director of Children’s Law Center Clinic & Assistant Professor of Law
KIMBERLY HAUSBEEK, B.A., J.D., LL.M.
Assistant Professor of Legal Writing

THOMAS E. HEARD, B.A., M.L.S., J.D.
Associate Professor of Library Services & Associate Director for Library Services
EMILY JANOSKI-HAEHLIN, B.S., J.D., M.L.S.
Assistant Professor of Library Services & Assistant Director for Research and Online Services
JENNIFER JOLLY-Ryan, B.A., J.D.
Professor of Legal Writing
KENNETH D. KATKIN, A.B., J.D.
Professor of Law
DONALD K. KAZEE, B.A., M.A., J.D.
Professor of Law
MICHAEL J.Z. MANNHEIMER, B.A., J.D.
Associate Professor of Law
BARBARA MCFARLAND
Director of Student Success Initiatives & Assistant Professor
LIUBOMIR NACEV, B.A., J.D., LL.M.
Professor of Law
ADRIENNE NOBLE NACEV, B.A., J.D.
Visiting Assistant Professor of Legal Writing
SHERRY PORTER,
Director for the Center for Excellence in Transactional Law
LARRY O. PUTT, B.A., J.D., LL.M.
Visiting Professor
DAVID SINGLETON, B.A., J.D.
Assistant Professor of Law
PHILLIP SPARKES, B.S., J.D., LL.M.
Assistant Professor of Law & Director of Chase Local Government Law Center
DONNA M. SPEARS, B.A., M.L.I.S., J.D.
Assistant Professor of Law Library Services & Assistant Director for Research and Instructional Technology
MARK M. STAVSKY, B.A., J.D., LL.M.
Professor of Law
HENRY L. STEPHENS, JR., B.A., J.D.  
Professor of Law

JOHN T. VALAURI, B.A., J.D.  
Professor of Law

CLAUDIA ZAHER, B.A., M.S.L.S.  
Associate Professor of Library Services  
Assistant Director for Collection Development

CARYL A. YZENBAARD, A.B., J.D.  
Professor of Law

EMERITI FACULTY

CAROL B. ALLRED, B.A., M.S.L.S., J.D.
ROBERT M. BRATTON, A.B., M.A., J.D.
EDWARD P. GOGGIN, J.D., LL.M.
W. JACK GROSSE, B.S.C., M.B.A., J.D.
MARTIN J. HUELSMAN, B.B.A., J.D.
WILLIAM R. JONES, B.S., M.A., J.D.
KAMILLA M. MAZENAC, A.B., J.D., LL.M.
FREDERICK SCHNEIDER, B.A., J.D.
ROBERT L. SEAVER, A.B., J.D.
DAVID C. SHORT, B.A., J.D., LL.M.

ADJUNCT FACULTY

SHARIF ABDRAHBO, B.S., J.D.
RAY ATKINSON, B.A., J.D.
DANIELLE ANDERSON, B.A., J.D.
HON. GREGORY M. BARTLETT, A.B., M.A., J.D.
HON. WILLIAM O. BERTELSMAN, B.S., J.D.
VICTORIA BOGGIS, B.A., J.D.
BRYANT BREWER, B.A., J.D.
LOUISE BROCK, B.A., J.D.
SHAWN P. BURTON
KELLY CANTRALL, B.A., J.D.
LISA DAVIDSON, B.A., J.D.
KRISTI DAVIDSON, B.A., J.D.
REBECCA DILORETO, B.A., J.D.
JOHN DUNN
SUSAN DUNN, B.S., J.D.
DOREENA FOX, B.S., J.D.
ROBERT A. GOERING, B.A., J.D.
HON. DANIEL T. GUIDUGLI, B.A., J.D.
WILLIAM GUSTAVSON, B.A., J.D.
MICHAEL HAWKINS, B.A., J.D.
PENNY HENDY
BILL HESCH, B.S., J.D.
M. GRETA HOFFMAN, B.S., J.D.
HON STEVEN R. JAEGGER, B.A., J.D.

RICHARD KATZ, B.A., J.D.
SHANNON KEMEN
JENNIFER LAWRENCE, B.S., J.D.
JENNIFER LEWIS
HENRY E. MENNINGER, B.A., J.D.
LAURIE MCClusKEY, B.S.N., J.D.
TIFANIIE McMillan, B.A., J.D.
JANET MOORE, B.A., M.A., M.A., J.D.
FRANK MUNGO, B.S., J.D.
DANIEL MURNER, B.A., J.D.
ELIZABETH PEARSON, B.A., J.D.
BRIAN POWELL
FINIS PRICE, B.A., J.D.
STEVEN RAY, B.A., J.D.
KEVIN ROONEY, B.A., J.D.
E. ROBERT SANDERS, B.A., B.S., J.D.
HON. AMUL THAPAR, B.S., J.D.
HON. KAREN A. THOMAS, B.A., J.D.
BERNADINE C. TOPAZIO, B.A., M.B.A., J.D.
MARY WAGNER, B.S./B.A., M.B.A., J.D.
HON. WILLIAM J. WEHR, B.A., J.D.
HON. J. GREGORY WEHRMAN, B.A., J.D.
DAVID WIELAN, B.A., J.D.
JUSTICE DONALD C. WINTERSHEIMER, A.B., M.A., J.D.
J. STEPHEN WIRTHLIN, JR., B.A., J.D.
2012 Law & Informatics Issue

ARTICLES

Implementing Procedural Safeguards for the Development of Bioinformatics Interoperability Standards
Jorge L. Contreras ................................................................. 87

The Emerging Conflict between Newsworthiness and the Right to be Forgotten
Jasmine E. McNealy .................................................................. 119

Digital Divisions: Racial (In)justice and the Limits of Social Informatics in the State of Georgia vs. Troy Anthony Davis
Mark Lawrence McPhail, Rachel Lyon, & David Harris ...................................................... 137

Datamining for Gold: Social Media and Social Capital in a Postnational Global Market
Susan H. Stephan ........................................................................ 163

Privacy and Confidentiality Issues in Historical Health Sciences Collections
Anne T. Gilliland and Judith A. Wiener ................................................................. 189

The Preoperational Legal Review of Cyber Capabilities: Ensuring the Legality of Cyber Weapons
P.J. Blount .................................................................................. 211

Playstation in Hot Water: Requiring Notice for Civil Discovery Pursuant to the Digital Millennium Copyright Act (DMCA) to Prevent John Doe Subpoenas from Boiling Over into First Amendment Violations
Andrea Laden ............................................................................ 221

Publicity Rights in India
Kalyan C. Kankanala and Sandeep Hegde M. .............................................................. 247

A Comparative Review of Cybercrime Law and Digital Forensics in Russia, the United States and under the Convention on Cybercrime of the Council of Europe
Galina Borisevich, Natalya Chernyadyeva, Evelina Frolova, Pavel Pastukho, Svetlana Polyakova, Olga Dobrovlyanina, Deborah Griffith Keeling, and Michael M. Losavio ........................................................................... 267

Regulating Human Subjects Research in the Information Age: Data Mining on Social Networking Sites
Lauren B. Solberg ........................................................................ 327
IMPLEMENTING PROCEDURAL SAFEGUARDS FOR THE DEVELOPMENT OF BIOINFORMATICS INTEROPERABILITY STANDARDS

Jorge L. Contreras*

I. INTRODUCTION

The field of bioinformatics, also referred to as computational biology, involves the use of computational methods to analyze large quantities of biological information. Bioinformatics was born as a distinct discipline in the mid-1990s when the Human Genome Project began to generate huge quantities of genomic data. Today, ever-increasing quantities of biological data are being generated by laboratories around the world. The stunning growth in this data and the multitude of research programs making use of it have led to urgent calls for standardized methods of storing, analyzing, and exchanging biological data.

In this respect, bioinformatics is not unique. Standards are ubiquitous in today’s technology-driven marketplace. Some standards mandate minimum requirements for product safety, others seek to reduce environmental impact, while others specify minimum levels of information that must be provided to consumers. “Interoperability standards,” which dominate the information, computing, and telecommunications (ICT) sector, specify the manner in which products and services offered by different vendors interact with one another. A number of these standards, including WiFi, USB, CD, DVD, PDF and HTML, have become household terms, and thousands of others ensure that a vast array of products and services connect and communicate seamlessly in a manner that is largely invisible to the consumer.

* Associate Professor of Law, American University, Washington College of Law. The author gratefully acknowledges research assistance by Chris Pepe.


3. AM. BAR ASS’N, ABA SECTION OF ANTITRUST LAW, HANDBOOK ON THE ANTITRUST ASPECTS OF STANDARDS SETTING 1 (2d ed. 2011) [hereinafter ABA ANTITRUST HANDBOOK].


7. ABA ANTITRUST HANDBOOK, supra note 1, at 9.
Standardization in the ICT sector, however, has not been achieved without a substantial cost. Over the past two decades, the industry has been plagued by lawsuits brought by participants in the standards-development process, and by government regulators and affected third parties. Two types of claims generally arise in standards-related litigation: process-abuse claims and patent hold-up claims. Process-abuse claims involve claims alleging that the standards process has been abused to disadvantage one or more companies, and also include claims that a participant in the standards-development process has improperly asserted its patents against an implementer of the standard. Standards-development organizations in the ICT sector have responded to these claims by promulgating rules and policies of increasing sophistication, both to specify procedures designed to avoid abusive activity and to accommodate the requirements of participants who control significant patent assets.

The explosion of bioinformatics research over the past two decades has led to a surge of interest in the development of interoperability and compatibility standards for bioinformatics applications. These standards range from genome annotation and controlled vocabularies (ontologies) to data formats and search engine integration. A variety of organizations are involved in standards-development activities. Involved organizations range from large, established standards bodies such as the Institute for Electrical and Electronics Engineers (IEEE)\(^8\) and the Worldwide Web Consortium (W3C),\(^9\) to broad-based bioinformatics industry associations such as the Asia-Pacific Bioinformatics Network\(^10\) and the European Bioinformatics Institute (EBI),\(^11\) to narrowly-focused efforts such as the Proteomics Standards Initiative (PSI)\(^12\) and the Functional Genomics Investigation Ontology (FuGO) project.\(^13\)

To date, the bioinformatics field has been blissfully free of the standards litigation that has plagued the ICT industry. But with the increasing adoption of standards by bioinformatics researchers and vendors, the issues faced by ICT standards groups will become increasingly relevant to bioinformaticists. I conducted an industry-wide study of bioinformatics standards-development activities and reviewed the policies and procedures adopted by each standards-development organization.\(^14\) The results of this study show that the majority of bioinformatics standards-development efforts are relatively informal and

---

unstructured. In many cases, these organizations either lack written policies entirely or adopt vague, aspirational statements regarding a desire that materials produced be “open” and publicly-available. This informal and minimalist approach not only invites abuse and opportunistic behavior, but also leaves aggrieved participants with little legal recourse after abusive behavior has occurred.

Accordingly, this Article recommends that bioinformatics standards-development organizations carefully review their existing policies and procedures. I recommend that these policies and procedures be revised to the extent that they fail to address key points regarding process and intellectual property. In order to assist organizations with this exercise, I offer a straightforward policy template that can be adapted to the specific requirements of particular bioinformatics standards organizations. Hopefully, these modest prophylactic measures will enable the bioinformatics standards community to continue to develop essential interoperability standards while avoiding the disruptive and costly litigation that has affected the ICT sector.

II. STANDARDS AND STANDARD SETTING: A BRIEF OVERVIEW

A. Types of Standards

Standards serve a variety of purposes and functions. Some standards specify requirements intended to protect public health and safety, to preserve the environment, and to prevent fraud and other abuses. These include standards relating to food and drugs, air and water quality, hazardous materials, construction, transportation, handling of personal data, and the like. Other standards signify a specified level of quality, such as the 4C (cut, color, clarity and carat) ratings for diamonds. Most relevant to bioinformatics, however, are interoperability or compatibility standards, which specify design features that enable data, materials, and services originated by different parties to operate together. Electrical outlets, for example, share a common design in the United States that enables any appliance to be plugged into any outlet anywhere in the country (though, as any frequent traveler knows, these standards vary dramatically from country to country). More complex, but equally illustrative, are the numerous networking (USB, WiFi, Bluetooth), Internet (TCP/IP, HTML, http), telecommunications (CDMA, GSM, LTE) and digital media (CD, DVD, BluRay) standards that enable devices manufactured by different vendors to interact with one another in a manner that is largely invisible to the consumer.

B. Mandatory and Voluntary Standards

At the highest level of generality, standards may be categorized as either mandatory, meaning that compliance is required by an external body, such as a governmental agency or a professional accreditation organization, or voluntary, meaning that compliance is not required, though it may be prudent or even
necessary from a commercial standpoint. Mandatory standards are often adopted by governments to protect the health and welfare of their citizens. Most interoperability standards, however, are voluntary.

C. Standards Development Organizations

Standards may be developed in a number of different environments. Individual companies may simply release a technology or format to the industry in the hope that it will become broadly adopted. Such “de facto” standards include Adobe Systems’ Portable Document Format (PDF) and Microsoft’s “.doc” document format. Other standards may be developed by a group of companies and institutions working collaboratively within a standards-development organization (SDO). SDOs vary greatly in size and composition. Some SDOs might consist of just a few participants that collaborate on a focused set of technical specifications, sometimes for a single product. These are sometimes referred to as consortia or “special interest groups” (SIGs). Standards for many consumer electronics devices and digital media such as the DVD disc and player were developed by SIGs. Other SDOs are very large and encompass many different standardization activities at any given time. ASTM International, for example, is one of the largest SDOs and regularly develops standards in areas as diverse as electrical wiring, playground equipment, composite materials, unmanned aircraft, and nanotechnology.

The work of individual SDOs is sometimes coordinated at the national and international levels. In the United States, SDOs can be accredited by the American National Standards Institute (ANSI) if they meet certain criteria of openness, due process, and transparency (“Essential Requirements”). The standards developed by ANSI-approved SDOs can be designated as American National Standards (ANS), a status that both validates and promotes adoption. More than 200 different SDOs are currently accredited by ANSI. The International Organization for Standardization (ISO) is a Geneva-based non-

---

15. For a more detailed overview of the standards-development landscape, see Brad Biddle, et al., The Expanding Role and Importance of Standards in the Information and Communications Technology Industry, 52 Jurimetrics 177, (2012), AMERICAN BAR ASSOCIATION, COMMITTEE ON TECHNICAL STANDARDIZATION, SECTION OF SCIENCE & TECHNOLOGY LAW, STANDARDS DEVELOPMENT PATENT POLICY MANUAL x-xi (Jorge L. Contreras, ed., 2007) (hereinafter “ABA PATENT POLICY MANUAL”).


19. Id.

governmental organization (NGO) whose members include 163 national standards institutes from across the globe.\footnote{Id.} ISO coordinates standards-development activities among its members and develops its own consensus standards through numerous committees.\footnote{Id.}

Many federal agencies also adopt standards, either as part of their regulatory function or for their own use. The Federal Office of Management and Budget’s (OMB) guidelines for federal agencies require that agencies adopt suitable “voluntary consensus standards” in their procurement and regulatory activities to the extent not “inconsistent with law or otherwise impractical.”\footnote{MEMORANDUM FROM THE U.S. OFFICE OF MGMT. & BUDGET TO THE HEADS OF EXECUTIVE DEPTS & AGENCIES, Circular No. A-119 Revised (Feb. 10, 1998), http://www.whitehouse.gov/omb/circulars_a119 [hereinafter OMB Circular A-119].} At an international level, the World Trade Organization’s (WTO) Uruguay Round Agreement on Technical Barriers to Trade requires that if recognized international standards exist with respect to a technical area, national governments developing standards in that area must adopt such international standards as the basis for their own national standards.\footnote{Final Act Embodying the Results of the Uruguay Round of Multilateral Trade Negotiations, Apr. 15, 1994, Agreement on Technical Barriers to Trade, Art. 2.4, 33 I.L.M. 1125 (1994), available at www.wto.org/english/docs_e/legal_e/03-fa.pdf.}

### III. The Bioinformatics Standards Landscape

Bioinformatics research utilizes a broad range of technologies including experimental apparatus such as microarrays, data analysis tools, and databases that store and allow sharing of experimental and analytic data.\footnote{A Science Primer, NATIONAL CTR FOR BIOTECHNOLOGY INFO. (2004), http://www.ncbi.nlm.nih.gov/About/primer/bioinformatics.html (last visited Jan. 30, 2012).} Standards are required within each of these broad technology categories to enable data sharing, analysis, and the interoperability of different experimental platforms.\footnote{Id.} To date, hundreds of standards relevant to bioinformatics applications have been developed in three broad categories: terminological artifacts, reporting requirements, and exchange formats.\footnote{This classification system was developed by Biosharing.org, which catalogs and provides information regarding most of the standards discussed below. See A Catalogue of Standards, BIOSHARING, http://www.biosharing.org/standards (last visited October 28, 2011). A list of the standards compiled by biosharing.org can be found at http://www.biosharing.org/standards_view.} Below is a brief description of these categories and a summary of some of the more prominent standardization efforts being undertaken in each.
A. Terminological Artifacts

A consistent and unambiguous vocabulary is required in order for different groups and applications to communicate about a wide array of organisms, experimental conditions, and study designs.28 A “controlled vocabulary” offers a single set of terms with explicitly-defined meanings within a particular field.29 An “ontology” creates relationships among these terms, often in hierarchical form,30 such as the familiar taxonomic classification for biological entities (kingdom, phylum, class, etc.).

One of the earliest and most mature bioinformatics ontologies is the Gene Ontology (GO), which has produced “a structured, precisely defined, common, controlled vocabulary for describing the role of genes and gene products in any organism.”31 The Gene Ontology Consortium, which developed the GO, began its work in 1998 as a joint project of research groups studying three different organisms (the fruit fly, budding yeast, and mouse).32 As of 2006, the GO included more than 1.6 million annotated gene products.33

Numerous other ontology projects have arisen following the success of the GO.34 These include the Systems Biology Ontology (SBO) originated by the European Bioinformatics Institute (EBI),35 the Open Biological and Biomedical Ontologies (OBO Foundry),36 and the Functional Genomics Investigation Ontology (FuGO) project.37

B. Reporting Requirements

The advent of microarray technology in the 1990s quickly led to the realization by the research community that standardized methods of reporting experimental data generated by microarray studies would be required. The Microarray Gene Expression Data (MGED) Society (now the Functional Genomics Data Society) was formed in 1999 by EBI to develop “Minimum Information About A Microarray Experiment” (MIAME), a checklist specifying

29. Id.
30. Id.
32. Id.
34. A more comprehensive list of ontology projects can be found in Chris F. Taylor, Standards for Reporting Bioscience Data: A Forward Look, 12 DRUG DISCOVERY TODAY 527, 529 (2007).
the information about every microarray experiment that should be reported in order to enable its proper validation, reproduction, and interpretation.38

Many other minimum information standards development efforts have followed the early success of MIAME.39 Among others, these include specifications for minimum information in hybridization and immunohistochemistry experiments (MISFISHIE),40 proteomics experiments (MIAPE),41 molecular interactions (MIMIx),42 and (meta)genome sequences (MIGS/MIMS).43 The Minimum Information for Biological and Biomedical Investigations (MIBBI) Project collects and publishes information about various minimum information standards.44

C. Exchange Formats

A recent compilation of molecular biology databases lists 1330 different data sources across the world.45 In order for researchers to make use of data beyond their own laboratories, they require the ability to access and utilize data from disparate sources. The exchange of data among different software applications and databases has become commonplace in today’s data-driven economy. Much of this exchange is accomplished using markup languages, or schema that enable the annotation of digital text in a manner that can be interpreted by a computer.46 The most common markup language, Hypertext Markup Language (HTML), is the dominant language for encoding web pages.47 Markup languages work through the use of “tags” that delimit characteristics of the text they designate.48 For example, in HTML, the tags <B> and </B> cause the text between the tags

---

38. See Catherine A. Ball & Alvis Brazma, MGED Standards: Work in Progress, 10 OMICS 138, 139-140 (2006).
39. There are more comprehensive lists of minimum information standards projects available: Taylor, supra note 58, at 528; Lyle D. Burgoon, Clearing the Standards Landscape: the Semantics of Terminology and their Impact on Toxicogenomics, 99 TOXICOLOGICAL SCIENCES 403, 408-10 (2007).
47. Id.
to be displayed in boldface type. Extensible Markup Language (XML), developed by the Worldwide Web Consortium (W3C), is a flexible data format that enables users to create customized tags based on the specific types of data in which they are interested.\textsuperscript{49} Hundreds of XML-based languages exist today, many of which are optimized for bioinformatics applications.\textsuperscript{50} Among the best-known XML-based bio-focused languages are the Systems Biology Markup Language (SBML),\textsuperscript{51} CellML for computational cell biology,\textsuperscript{52} MAGE-ML, for the exchange of microarray data,\textsuperscript{53} and BioPAX, for the exchange of biological pathway data.\textsuperscript{54}

Despite the widespread adoption of XML as the preferred standard for data exchange in the biosciences, some commentators have criticized XML as too limited and imprecise for the robust exchange of scientific data.\textsuperscript{55} An alternative data exchange standard is the Reference Data Format (RDF), also developed by W3C, which takes advantage of the so-called “semantic web” and offers developers greater freedom to define data relationships.\textsuperscript{56} The Bio2RDF Project led by W3C has recently developed software and a website for accessing data from different public bioinformatics databases in RDF format.\textsuperscript{57}

Closely related to markup languages are object models. Object models describe the relationships among computer programming “objects” of interest within a given discipline and can thus act as blueprints for the development of specialized markup languages.\textsuperscript{58} Of particular interest in bioinformatics are the Microarray and Gene Expression Object Model (MAGE-OM),\textsuperscript{59} the SysBio-OM developed by the National Institute of Environmental Health Sciences


\textsuperscript{50} More comprehensive lists of bioinformatics markup languages can be found in Burgoon, supra note 63, at 409; Luciano Milanesi, Trends in Modeling Biomedical Complex Systems, 10 BMC BIOINFORMATICS, 12 (Supp. 2009).


\textsuperscript{53} See Ball & Brazma, supra note 62, at 140-41.


\textsuperscript{55} See, e.g., John Quackenbush, Standardizing the Standards, 2 MOLECULAR SYSTEMS BIOLOGY 1, 1-2 (2006); Xiaoshu Wang et al., From XML to RDF: how semantic web technologies will change the design of 'omic' standards, 23 NATURE BIOTECHNOLOGY 1099 (2005).

\textsuperscript{56} Wang, supra note 79, at 1099.

\textsuperscript{57} See Francois Bellau et al., Bio2RDF: Towards a Mashup to Build Bioinformatics Knowledge Systems, 41 J. BIOMEDICAL INFORMATICS 706 (2008).


The object models and markup languages discussed above are essential for the exchange of data among disparate data sources and databases. Yet data exchange tools alone are not enough, and commentators find that the proliferation of incompatible data sources has led to increasing duplication of effort, poor interoperability, and loss of data. To address these problems, an international consortium of database users and developers has begun work on a uniform set of defining attributes for biological databases called BioDBCore.

IV. COMPETITION AND ANTITRUST ISSUES FOR STANDARDS DEVELOPERS

One of the principal purposes of antitrust law is to prevent competitors from colluding in ways that are harmful to competition and the market. Such collusive behavior in the U.S. is typically prosecuted under Section 1 of the Sherman Act, which broadly prohibits agreements in restraint of trade. In recent years, the Federal Trade Commission (FTC) has also exercised its authority under Section 5 of the FTC Act to prosecute unfair methods of competition and unfair trade practices that arise in the standards-setting context. Because consensus-based technical standards are generally developed through collaborative processes that involve multiple competitors, having a basic understanding of antitrust law principles is critical to effective operation of any standards-development organization. This section summarizes some of the major antitrust and competition issues that can arise in the standards-setting context.

A. Improper Exclusion

SDOs must exercise caution if they wish to limit their membership or to expel a member after it has joined. The exclusion of parties from the standard-setting process can be viewed as an attempt by the SDO members to gain an unfair advantage over the excluded parties. Accordingly, many SDOs do not restrict their membership and claim to be open to all interested participants. Being “open,” however, does not mean that an SDO must admit all participants on equal terms. It is not uncommon, for example, for SDOs to vary their...
membership fees based on a participant’s size, revenue, or industry sector (e.g., producer, customer, government, academic, etc.). Courts have also held that trade associations may establish reasonable criteria for membership, even if such criteria necessarily exclude some potential participants, many important industry standards, such as the CD and DVD digital storage formats were developed by small, closed groups of industry participants. Although some limitations may be permitted, SDOs can avoid many allegations of improper exclusion by opening their membership as broadly as possible. Similar issues regarding exclusion arise when a group wishes to expel a member. In short, expulsion of a member is generally permissible when the member has violated the organization’s rules or otherwise acted in an unlawful or unethical manner.

Claims of anticompetitive exclusion can arise in connection with technologies as well as participants. Thus, even if a company is not excluded from participation in an SDO, it is possible for other SDO participants to collude to exclude that company’s technology from a standard under consideration. Such claims were raised, for example, by Addamax Corporation in Addamax Corp. v. Open Software Foundation Inc. Addamax was a developer of security software for the UNIX operating system. Open Software Foundation (OSF), a consortium of computer and software vendors, developed a version of UNIX that included a security package developed by one of Addamax’s competitors. Addamax alleged, among other things, that OSF’s exclusion of its security software from OSF UNIX amounted to unfair competition and a boycott of Addamax’s products by the members of OSF. After a lengthy litigation, the First Circuit rejected these claims, holding that Addamax failed to show that the eventual decline in sales of its security products was attributable to concerted action by OSF and its members.

68. Id.

69. Nat’l Ass’n of Review Appraisers & Mortg. Underwriters v. Appraisal Found., 64 F.3d 1130, 1133 (8th Cir. 1995) (upholding Appraisal Foundation’s membership criteria where there was no evidence of any harm to the overall market for appraisal organizations).

70. See, e.g., Pretz v. Holstein Friesian Ass’n of Am., 698 F. Supp. 1531, 1542 (D. Kan. 1988) (holding that cattle registry association did not commit antitrust violation by expelling a member alleged to be manipulating tests for grading cattle).


72. Id. at 49.

73. Id. at 50.

74. Id.

B. Improper Exchange of Information

If competitors exchange sensitive commercial information during standard-setting meetings, or if they otherwise use the standard-setting process as a vehicle for engaging in illegal collusion, the SDO can be challenged for facilitating this unlawful behavior. The clearest example of behavior exposing SDOs to potential antitrust risk is the sharing of information relating to product pricing or salaries. But less blatant instances of information sharing may also lead to allegations of anticompetitive behavior. For example, a standard could facilitate collusion by making it easier for competitors to monitor and enforce illegal price fixing agreements. Likewise, a real estate SDO’s bylaws and policies could facilitate collusion among members by prohibiting a broker from conveying a listing to his customers via the Internet without permission of the listing broker.

C. Compliance Certification

In some cases, the members of an SDO may improperly influence the SDO’s decisions regarding whether a competitor’s products comply with a standard. The Supreme Court addressed this type of behavior in *American Society of Mechanical Engineers v. Hydrolevel Corp.* In that case, a subcommittee chair of the American Society of Mechanical Engineers (ASME), an SDO with over 90,000 members, misrepresented that Hydrolevel’s boiler control valves did not conform to a key provision of ASME’s Boiler and Pressure Vessel Code, and were therefore unsafe. He allegedly made these misrepresentations because his employer competed with Hydrolevel in the boiler control valves market. When ASME staff further propagated this inaccurate portrayal, Hydrolevel suffered significant harm in the market. The Supreme Court held that the SDO could be liable for these misrepresentations, as the weight of its reputation greatly enhanced the anticompetitive effect of its member’s misrepresentation.

---

76. See, e.g., United States v. Container Corp. of Am., 393 U.S. 333, 337 (1969) (holding that exchange of price quotes for sales of corrugated containers was a price fixing agreement that violated the Sherman Act since the product was fungible and demand was inelastic); Todd v. Exxon Corp., 275 F.3d 191, 214-15 (2nd Cir. 2001) (holding that employees have a claim against employers to examine employers’ habit of sharing information regarding non-managerial, non-union workers to determine if it is was a collusion to keep wages down in violation of the Sherman Act).
80. Id. at 558-562.
81. Id. at 560.
82. Id. at 562.
83. Id. at 577.
But not all allegations that an SDO improperly failed to certify a product’s compliance with its standards are successful. In Consolidated Metal Products v. American Petroleum Institute, the plaintiff alleged that the American Petroleum Institute (API) committed an antitrust violation by intentionally delaying certification of its products. The Fifth Circuit rejected this claim, holding that the plaintiff did not have a claim “simply because others refuse to promote, approve, or buy its products.”

D. Abuse of Process

Perhaps the most frequent antitrust charge against SDOs is the claim that one or more participants abused the process by which standards are set within the SDO, either to secure approval of a standard that they backed or to exclude the technology of their competitors from a standard. The Supreme Court famously addressed this type of abuse in Allied Tube & Conduit v. Indian Head. In that case, the plaintiff, a manufacturer of polyvinyl chloride (PVC) products, requested that the National Fire Protection Association (NFPA) approve an amendment to the National Electrical Code that would have allowed the use of PVC in electrical wiring conduits. The defendant, a manufacturer of steel conduit, recruited 230 people to join NFPA for the sole purpose of voting against the amendment, which was ultimately defeated by a vote of 394 to 390. The jury found that the steel conduit manufacturers defeated the PVC standard solely for anticompetitive purposes, subverting the standards-development process and violating the antitrust laws. The Supreme Court agreed, stating that a participant in private standards-setting activities should not bias the process in a manner designed to restrain competition.

E. Policies and Precautions

In order to avoid the antitrust claims discussed above, as well as the undesirable conduct by participants that led to such claims, SDOs have increasingly adopted rules and policies that expressly prohibit anticompetitive behavior within the SDO context. Such policies typically seek to accomplish the following general objectives:

85. Id. at 286.
86. Id. at 293; See generally ABA HANDBOOK, supra note 1, at 55-59.
88. Id. at 496.
89. Id. at 496-97.
90. Id. at 498.
91. Id. at 511.
a. to ensure that the standards-development process is open, fair, and transparent;
b. to ensure that membership in the SDO is open to all interested parties on
   a non-discriminatory basis;
c. to prohibit the sharing of competitive information within the context of
   SDO activities; and

d. to provide that compliance with standards is voluntary, and that
   participation in the SDO is not conditioned on use of the SDO’s output.

While policies implementing these objectives cannot themselves prevent
   collusion or improper behavior by SDO participants, they can serve to raise
   awareness of antitrust issues within the SDO. More importantly, such policies
   can demonstrate (whether to potential plaintiffs or finders of fact) that the SDO
   has actively sought to curtail activity that could be construed as anticompetitive.

V. INTELLECTUAL PROPERTY AND STANDARDS

Standards often implicate and are affected by intellectual property. Indeed,
   standards themselves may specify patentable inventions, and the written
   embodiments of standards are generally protectable by copyright. Furthermore,
   the more complicated the technology that a standard specifies, the more likely
   the standard is to implicate patents owned by members of the SDO or by third
   parties. SDOs and implementers of technical standards are therefore likely to
   encounter numerous intellectual property issues outlined in this section.

A. Copyright in Standards

Technical standards typically take the form of written descriptions of how
   products or services should be designed, built, or operated.93 Similar to written
   documents, standards are typically protected by copyright, meaning that they
   cannot be reproduced, displayed, or modified without permission of the
   copyright owner (often the SDO).94 Many SDOs earn significant revenue from
   the sale of standards (some of which extend to hundreds of pages) and therefore
   warn against illegal copying and distribution,95 though a number of major SDOs
   allow their standards to be downloaded and copied without charge.96 The
   tension between copyright protection and the social utility of standards becomes
   particularly clear when a proprietary standard is adopted and referenced by a

93. Lemley, supra note 31, at 1896.
94. See, e.g., INT’L ORG. FOR STANDARDIZATION AND INT’L ELECTROTECHNICAL COMM’N,
iso/copyright_information_brochure.pdf.
95. Id.
96. See, e.g., Legal Provisions Relating to IETF Documents, IETF TRUST, § 3, Dec. 28, 2009,
governmental agency, thereby becoming “the law.” Use of a copyrighted standard might become mandatory by statute or regulation, yet access to that standard can be controlled by the SDO that owns the copyright.

Such a situation led to litigation when the federal Health Care Financing Administration (HCFA) required the use of the Current Procedural Terminology (CPT) standard for Medicare and Medicaid reimbursement claims. The copyright in this standard was owned by the American Medical Association (AMA), which granted HCFA “a non-exclusive, royalty free, and irrevocable license to use, copy, publish, and distribute” the standard. In Practice Management Information Corp. v. American Medical Ass’n, Practice Management Information (PMI), an independent publisher, desired to publish the CPT standard. Arguing that the CPT standard was now incorporated in federal regulation, PMI sought a declaratory judgment that the AMA’s copyright in the CPT standard was no longer valid. The U.S. Court of Appeals for the Ninth Circuit, however, declined to invalidate the AMA’s copyright, holding instead that the AMA controls the copyrighted text of the CPT standard, even after it was adopted into law. This approach is consistent with the OMB’s guidance to federal agencies, which states that agencies adopting voluntary consensus standards “must observe and protect the rights of the copyright holder.”

However, the Court of Appeals for the Fifth Circuit has taken a different approach with respect to the issue of copyright in legally-mandated standards. In Veeck v. Southern Building Code Congress Intl, Peter Veeck, the operator of a non-profit web site, posted the local building codes of two Texas municipalities. The codes were taken verbatim from Southern Building Code Congress International’s (SBCCI) published Standard Building Code. When Veeck published the codes on his web site, SBCCI sued him for infringement of...
its copyrights. The *en banc* Fifth Circuit, relying on precedent that copyright cannot prevent the reproduction and distribution of “the law,” held that while SBCCI retains the copyright in its model codes, the codes may be reproduced and distributed freely once enacted into law. Important to the court’s reasoning was the fact that SBCCI’s model codes were developed specifically for the purpose of being adopted by municipalities and incorporated into their local building codes. The court distinguished this case from one in which a governmental agency simply references an existing standard in its regulations.

In such a case, the court suggested that it would not be unreasonable to permit the authoring SDO to continue charging for access to its standard, notwithstanding its incorporation in such regulations.

The debate regarding incorporation of published standards into legislative material has recently gained renewed attention following a February 2012 petition by Professor Peter Strauss of Columbia Law School (together with several other academics and public interest advocates) seeking to amend the authorizing regulations for the Federal Register to require that technical standards referenced in federal regulations be made available via the Internet. The petition has generated significant debate, and responses to a subsequent Federal Register request for comments have both supported and opposed the proposed amendment.

B. Patenting and Standards

1. Patents Covering Standardized Technology

As noted above, standards are written descriptions of particular attributes of specified products and processes. Assuming that statutory requirements of

110. Id. at 794.
111. Id. at 800.
112. Id. at 803.
113. Id. at 804.
114. Id.; See also, CCC Info. Serv. v. Maclean Hunter Mkt. Reports, Inc., 44 F.3d 61 (2nd Cir. 1994); Practice Mgmt. Info. Corp., 121 F.3d at 516.
116. See, e.g., Letter from Michael Hertz to Hon. Cass Sunstein, Administrator, Office of Information and Regulatory Affairs dated June 1, 2012 (submitted on behalf of the ABA Section of Administrative Law).
utility, novelty, and non-obviousness are met, patents may be obtained on bioinformatics products and processes that conform with particular standards. Such a patent would ordinarily not be obtained by the SDO in which the standard was developed, as SDOs seldom develop complete products and almost never seek to patent their work. Rather, if such a patent were obtained, it would be obtained by a participant in the SDO or an outsider, and sometimes both. Thus, two general patent-related issues arise in the context of technology standardization: “patent stacking” and “patent hold-up.”


Patent or royalty “stacking,” also referred to as a patent “thicket” or anti-commons, occurs when multiple entities each hold patents claiming aspects of a single standardized technology.\(^\text{118}\) In order for a producer to implement the standardized technology in a product, it must obtain licenses from multiple parties, each acting independently and each seeking to maximize its gains.\(^\text{119}\) The risk of stacking is that the sum of individual royalty demands may be excessive in relation to the overall value of the product, making the standardized product uncompetitive in comparison to products that do not conform with the standard.\(^\text{120}\)

One method of addressing patent stacking is through the creation of a patent pool. In a patent pool, multiple patent owners contribute or license patents that are essential to the implementation of the standard to a common agent (sometimes one of the patent holders and sometimes a newly-formed entity). Licensees are charged a single royalty to practice the entire group of patents, and net revenues are allocated among the pool participants in accordance with a pre-determined formula. Such pools have been used effectively in consumer electronics standards such as the MPEG audio compression format,\(^\text{121}\) the DVD video compression format,\(^\text{122}\) and third generation wireless communications


\(^{119}\) Lemley & Shapiro, supra note 155, at 1993.


standards. In each of these instances the U.S. Department of Justice approved the proposed patent pool, so long as it possessed certain features that would reduce potentially anticompetitive effects. For example, pools must contain only patents “essential” to the implementation of the standard (as the inclusion of patents on substitute technologies could lessen competition among technical alternatives). Furthermore, licensees must have the freedom to obtain licenses to the patents independently from the pool, and licensing of the pooled patents must be conducted on a non-discriminatory basis. To the extent that the patent pool owners require licensees to “grant back” licenses to them, such grantback licenses must only cover patents that are, themselves, essential to implementation of the standard.

It is important to note that the usefulness of a patent pool may be limited if fewer than all holders of essential patents participate. This situation arose recently in connection with the Federal Communication Commission’s (FCC) mandatory ATSC digital television standard. Though several holders of patents essential to the ATSC standard formed a patent pool, one patent holder, Japan’s Funai Electric Company, did not join. Instead, Funai sought to charge royalties for a single patent at a rate allegedly equal to the rate charged by the entire ATSC pool. Vizio, Inc., a U.S. television manufacturer, refused to pay this royalty, causing Vizio to seek relief from the FCC. Though the matter was ultimately rendered moot when the Federal Circuit held that Vizio did not infringe the asserted patent, the dispute highlights the limited benefits of of patent pooling arrangements that do not include all holders of standards-essential patents.

3. Patent Ambush

The second major patent issue that can arise in the standards context is patent ambush. Patent ambush occurs when a patent holder seeks to assert a previously unidentified patent against implementers of a standard after the standard has been adopted (either by an SDO or a governmental agency). If
patent ambush occurs after the industry has devoted significant resources to production, marketing, and training with respect to standardized products (in economic terms, after the standard has become “locked-in”), unexpected royalty demands from patent holders can have an extremely disruptive effect on the market. This phenomenon is commonly referred to as “hold-up” and results in an increase in the cost of standardized products, sometimes to levels that are inefficient and uncompetitive with alternative technologies.135

Patent ambush has been alleged in several cases within the ITC industry. The first of these cases to gain significant attention involved Dell Computer, which allegedly failed to disclose patents covering the voluntary VL-bus standard that it helped to develop at the Video Electronics Standards Association (VESA).136 Following approval of the standard, Dell sought to enforce its patents against other computer manufacturers. Responding to complaints by these potential infringers, the Federal Trade Commission (FTC) sought to enjoin Dell’s enforcement activity on the ground that Dell’s violation of the VESA disclosure rule effectively rendered its patents unenforceable.137 The FTC action resulted in the entry of a 1996 consent order that permanently prohibited Dell from enforcing its VL-bus patents against any third party.138

Perhaps the most notorious case of disclosure failure within an SDO involved Rambus, Inc., a developer of semiconductor memory technology. Volumes have been written about the decade-long legal battles in which Rambus sought to assert its patents against implementers of dynamic random access memory (DRAM) technology standardized by the Joint Electron Device Engineering Council (JEDEC), a voluntary SDO in which Rambus participated in the early 1990s.139 Despite conduct that was condemned by both the Court of Appeals for the Federal Circuit and the FTC, Rambus was largely exonerated on the basis that the poorly-worded JEDEC patent policy was simply too imprecise...


135. See Lemley, supra note 134, at 154-55 and FTC 2011 Report at 5 (“[a]t the time a manufacturer faces an infringement allegation, switching to an alternative technology may be very expensive if it has sunk costs in production using the patented technology. ... If so, the patentee can use the threat of an injunction to obtain royalties covering not only the market value of the patented invention, but also a portion of the costs that the infringer would incur if it were enjoined and had to switch. This higher royalty based on switching costs is called the “hold-up” value of the patent. Patent hold-up can overcompensate patentees, raise prices to consumers who lose the benefits of competition among technologies, and deter innovation by manufacturers facing the risk of hold-up”).


137. Id.

138. Id.

an instrument to support liability.\textsuperscript{140} The court criticized the JEDEC policy as suffering from “a staggering lack of defining details” that left SDO participants with “vaguely defined expectations as to what they believe the policy requires.”\textsuperscript{141}

In a subsequent action, the FTC found Rambus liable for, among other things, attempted monopolization in violation of Section 2 of the Sherman Act and deceptive conduct under Section 5 of the FTC Act.\textsuperscript{142} The FTC’s decision, however, was reversed by the Court of Appeals for the D.C. Circuit, which held that Rambus’s attempt to increase prices following adoption of a standard could not amount to anticompetitive conduct unless such conduct also resulted in adoption of the standard, which was not shown.\textsuperscript{143} This decision has been criticized, both on the basis of its antitrust analysis and as a matter of public policy, inasmuch as it failed to sanction conduct that was widely condemned as deceptive.\textsuperscript{144}

C. SDO Patent Policies

1. Policy Measures to Address Patent Issues

The Dell and Rambus cases demonstrated to the standards-development community both that patent ambush was a real possibility, and that existing SDO policies might lack adequate force to prevent such conduct. In response, many SDOs adopted or enhanced their formal policies to address ambush issues more clearly.\textsuperscript{145} They did so by imposing one or both of the following obligations on SDO participants: (1) an obligation to disclose patents essential to implementation of a standard, and/or (2) an obligation to license patents essential to implementation of a standard, either on a royalty-free basis or on terms that are “reasonable and nondiscriminatory.”\textsuperscript{146} Such obligations are intended to

\textsuperscript{140} Id.
\textsuperscript{141} Id. at 1102.
\textsuperscript{143} Rambus, Inc. v. F.T.C., 522 F.3d 456, 463 (D.C. Cir. 2008), cert. denied 129 S.Ct. 1318 (2009).
\textsuperscript{145} Patent ambush can involve either patents held by participants in the SDO or patents held by non-participating third parties. The risk posed by SDO participants’ patents is perceived as particularly serious, however, because, unlike non-participating third parties, SDO participants can potentially shape the technical parameters of a standard toward their own patent positions. See Royall, supra note 174, at 34; Lemley, supra note 174, at 152.
ensure that standards developers have sufficient information to assess the relative costs and risks of technologies under consideration for standardization. That is, disclosure obligations ensure that standards developers know whether and which patents cover technologies under consideration, giving them the opportunity to “design around” such patents if they so wish.\textsuperscript{147} Likewise, licensing obligations are intended to ensure that such patents will be licensed to implementers of the standard on terms that are, at least roughly, understood.\textsuperscript{148}

2. Royalties for Standards-Essential Patents

Many SDO policies require that participants license patents essential to their standards on terms that are “reasonable and non-discriminatory” (RAND) or “fair, reasonable and non-discriminatory” (F/RAND).\textsuperscript{149} This requirement is built into ANSI’s “Essential Requirements” for all ANSI-accredited SDOs\textsuperscript{150} and is equally pervasive in Europe and other jurisdictions.\textsuperscript{151} Despite the intuitive appeal of these requirements, however, a consistent and practical definition of F/RAND terms has proven difficult to develop.\textsuperscript{152} In several recent cases, parties have disputed whether the terms under which licenses have been proffered violate or conform with F/RAND requirements.\textsuperscript{153}

F/RAND licensing commitments tend to fail because there is no universal, objective standard by which “reasonableness” (or “nondiscrimination”) can be measured.\textsuperscript{154} In order to make a F/RAND determination, the specific facts of each situation must be evaluated.\textsuperscript{155} These facts include not only relevant market norms for royalties, but also customary practices relating to non-royalty terms such as reciprocity, grantback licenses, defensive suspension, confidentiality, and the like.\textsuperscript{156} Also, given that a patent holder’s F/RAND licensing terms are generally not revealed until negotiations that occur after a standard has been adopted (i.e., “locked-in”), parties involved in standards setting can experience
uncertainty regarding the ultimate cost of adopting a standard encumbered by patents.\textsuperscript{157} Put another way, the uncertainty of F/RAND licensing may simply substitute the risk of patent hold-up arising from unknown patents with hold-up arising from unknown F/RAND licensing terms.\textsuperscript{158}

3. Ex Ante Disclosure of License Terms

Several commentators have suggested that permitting or requiring patent holders to disclose their royalty rates and licensing terms to SDO participants prior to the adoption of a standard (i.e., “ex ante”) would alleviate the F/RAND hold-up problems described above.\textsuperscript{159} Such advance disclosure would enable SDO participants to evaluate the cost of including particular patented technologies in a standard prior to adoption, and would thus enable more efficient decision making with respect to the technical design of the standard.\textsuperscript{160}

Critics, however, have argued that \textit{ex ante} disclosures in the standards context might cause the standardization process to become more cumbersome, lengthy, and expensive.\textsuperscript{161} However, a recent empirical study of the effects of \textit{ex ante} disclosure of licensing terms on SDOs that have adopted \textit{ex ante} disclosure policies found no evidence linking such policies to reductions in the number of standards adopted, the speed of standardization, the quality of standards, or the levels of royalties charged.\textsuperscript{162} Concerns have also been raised that allowing \textit{ex ante} licensing negotiations could facilitate the improper exchange of information among competitors and might place too much power in the hands of licensees acting collectively.\textsuperscript{163} That is, potential implementers of a standard, in negotiating \textit{ex ante} license terms with a patent holder, could collectively exert anticompetitive pressure on the patent holder, causing royalties to decrease below their fair (or optimal) level.\textsuperscript{164} Following this argument to its logical

\textsuperscript{157} Id.
\textsuperscript{160} Wallace, supra note 186, at 690.
\textsuperscript{161} DOJ/FTC Report, supra note 157, at 50; Skitol, supra note 204, at 734.
\textsuperscript{163} See 2007 DOJ/FTC Report, supra note 157, at 52.
\textsuperscript{164} See 2007 DOJ/FTC Report, supra note 157, at 52-53; Skitol, supra note 204, at 735.
conclusion, group pressure could drive all royalty rates toward zero, resulting in the devaluation of any patents covering a standard.

Despite these considerations, the U.S. Department of Justice (DOJ) has on two recent occasions issued Business Review Letters approving limited ex ante disclosure policies in SDOs. In the case of the VMEbus International Trade Association (VITA), the DOJ indicated in 2006 that it would not take enforcement action against an SDO that required participants to make ex ante declarations of the “most restrictive” licensing terms in their RAND licenses. In approving the VITA policy, the DOJ concluded that ex ante disclosure of restrictive licensing terms would promote, rather than hinder, competition among patent holders. Likewise, in its 2007 Business Review Letter to IEEE, the DOJ approved a proposed arrangement in which patent holders were given the option to disclose their most restrictive licensing terms, including royalty rates, prior to the adoption of a standard. The DOJ called the IEEE proposal “a sensible effort to preserve competition between technological alternatives before the standard is set in order to alleviate concern that commitments by patent holders to license on RAND terms are not sufficient to avoid disputes.” The European Commission has also expressed a general level of comfort with ex ante licensing disclosures in its guidelines relating to horizontal competition.

VI. BIOINFORMATICS STANDARDS POLICIES TODAY: ASSESSMENT AND RECOMMENDATIONS

A. Summary of Bioinformatics SDO Policies

Technical standards are likely to play an increasingly prominent role in the development, adoption, and regulation of bioinformatics research and technologies. Whether such standards relate to minimum information requirements, controlled vocabularies, or data exchange formats, the legal and policy considerations described in this section will play a key role in determining which of these standards are broadly adopted, and at what price.

166. Id.
168. Id.
169. Id.
171. Admittedly, intellectual property considerations may play a smaller role in standards devoted to the definition of controlled vocabularies and minimum information guidelines (which are themselves less amenable to patent protection) than they do in standards relating to data.
Given the importance of legal issues to standards development in other sectors of the economy, we conducted a review of the publicly-available policies and rules of a number of major bioinformatics standards initiatives. The results, summarized in Table 1 below, indicate that few standardization efforts in bioinformatics address these issues in detail, and a significant number omit any legal guidelines in their public documentation.

Table 1
Summary of Selected Bioinformatics SDO Policies

<table>
<thead>
<tr>
<th>Standards-Development Organization (SDO)</th>
<th>Year Started</th>
<th>Notable Standards</th>
<th>Type</th>
<th>Antitrust Guidelines</th>
<th>Intellectual Property policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asia-Pacific Bioinformatics Network172</td>
<td>1998</td>
<td>Minimum Information About a Bioinformatics Investigation</td>
<td>Reporting</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>BioPAX.org 173</td>
<td>2002</td>
<td>BioPAX</td>
<td>Exchange</td>
<td>None</td>
<td>Open source licenses that are academic and corporate friendly are used for all work created by the group</td>
</tr>
<tr>
<td>European Bioinformatics Inst. (EBI)174</td>
<td>1992</td>
<td>Systems Biology Ontology (SBO)</td>
<td>Terminology</td>
<td>None</td>
<td>No restrictions on the use or redistribution of data. Some original data may be subject to patent, copyright, or other intellectual property rights, and users must ensure that their exploitation of the data does not infringe the rights of such third parties</td>
</tr>
<tr>
<td>Functional Genomics Investigation Ontology (FuGO) project175</td>
<td>2006</td>
<td>Functional Genomics Investigation Ontology (FuGO)</td>
<td>Terminology</td>
<td>None</td>
<td>None</td>
</tr>
</tbody>
</table>

exchange formats, database structures, and scientific apparatus. This distinction may be less pronounced with respect to the impact and importance of antitrust issues.

<table>
<thead>
<tr>
<th>Standards-Development Organization (SDO)</th>
<th>Year Started</th>
<th>Notable Standards</th>
<th>Type</th>
<th>Antitrust Guidelines</th>
<th>Intellectual Property policy</th>
</tr>
</thead>
</table>
| Functional Genomics Data Socy. (FGED) [formerly Microarray Gene Expression Data (MGED) Socy.]
| 1999                                   | MGED Ontology | Minimum Information About a Microarray Experiment (MIAME) | Terminology Reporting | None                  | No funding sources have IP rights over FGED’s output; FGED currently owns no patents or copyrights, and advocates free use of data, tools, and publications |
|                                        | Minimum Information Specification For In Situ Hybridization and Immunohistochemistry Experiments (MISFISHIE) |                               | Reporting |                  |                             |
|                                        | MAGE-ML       | Exchange          |               | None                  |                             |
| Genomic Standards Consortium (GSC)      | 2005          | Minimum Information about a MARKer gene Sequence standard (MIMARKS) | Reporting | None | GSC utilizes Common Public License Version 1.0 (CPL). The license generally provides that any contributor grants a royalty free license to use any copyrighted or patented materials that he/she contributes |
| Intl. Socy. Biocuration                | N/A           | BioDBCore         | Reporting | None | None |
| Gene Ontology Consortium (GOC)         | 1998          | Gene Ontology     | Terminology | None | Unrestricted use if user acknowledges GO as source, displays the version number, and does not alter files |
| Metabolomics Standards Initiative (MSI) | 2005          | Core Information for Metabolomics Reporting (CIMR) | Reporting | None | Working group output is fully available to public |

<table>
<thead>
<tr>
<th>Standards-Development Organization (SDO)</th>
<th>Year Started</th>
<th>Notable Standards</th>
<th>Type</th>
<th>Antitrust Guidelines</th>
<th>Intellectual Property policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>OBO Foundry(^{181})</td>
<td>2001</td>
<td>Does not create its own, but endorses ontologies that meet its principles and standards</td>
<td>Terminology</td>
<td>None</td>
<td>OBO will not endorse ontology unless it allows for free use to all</td>
</tr>
<tr>
<td>Proteomics Standards Initiative (PSI) [HUPO](^{182})</td>
<td>2002</td>
<td>Minimum Information about a Proteomics Experiment (MIAPE)</td>
<td>Reporting</td>
<td>None</td>
<td>PSI takes no position regarding validity or scope of any IP or other rights pertaining to the implementation or use of technology or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any effort to identify any such rights</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Min. Information about a Molecular Interaction Experiment (MIMIx)</td>
<td>Reporting</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Min. Information about a Protein Affinity Reagent (MIAPAR)</td>
<td>Reporting</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Proteomics Standards Initiative-Molecular Interaction (PSI-MI) XML</td>
<td>Exchange</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>mZML</td>
<td>Exchange</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SBML.org(^{183})</td>
<td>2000</td>
<td>Systems Biology Markup Language</td>
<td>Exchange</td>
<td>None</td>
<td>The organization considers SBML to be free and open to the community, such that no one owns rights to it</td>
</tr>
<tr>
<td>University of Auckland(^{184})</td>
<td>2004(^{185})</td>
<td>CellML</td>
<td>Exchange</td>
<td>None</td>
<td>Individuals may freely use, publish and redistribute CellML; write and sell applications which create, load, or write CellML-valid XML files; distribute or sell their own CellML-valid XML files; and transmit verbatim copies of the CellML format to any person without restriction</td>
</tr>
</tbody>
</table>


\(^{185}\) Work on CellML began in 2004. The University itself is much older.
As shown in Table 1, in many cases the organizations responsible for bioinformatics standards development either lack written policies entirely or have adopted vague, aspirational statements regarding a desire that materials produced be “open” and publicly-available. This informal and minimalist approach not only invites opportunistic behavior, but also leaves aggrieved participants with little legal recourse after abuse has occurred.

Nevertheless, the data collected in Table 1 does reveal a number of recurring themes. These include a general preference that bioinformatics standards be “open” and “not restricted” by intellectual property rights. Stated more precisely, these preferences can be expressed in terms of the following two maxims: (a) bioinformatics standards should be freely available, and (b) the implementation of bioinformatics standards should not be impeded by patent holders.

B. Policy Recommendations

As discussed above, it is important for SDOs to establish clear policies regarding compliance with antitrust law and the disposition of intellectual property rights in a manner that is aligned with the expectations and wishes of their participants. At a minimum, such policies should include provisions addressing the antitrust considerations described in Section IV.E above, as well minimum provisions relating to copyrights and patents. Among the more critical issues to include in such policies are the following:

Copyrights
1. What rights do SDO participants grant to the SDO and to one another with respect to their copyrights in documents, text and code that have been “contributed” to a standard?
2. Is the standard available free of charge, or must those wishing to implement it purchase copies from the SDO or others? If the latter, do SDO participants gain access at a discounted rate?
3. What rights does the SDO grant to the world under its copyrights, if any, in a standard (e.g., can the standard be reproduced, modified, translated,

---

excerpted, or otherwise manipulated outside of the SDO that developed it)?

Patents
1. May SDO participants obtain patents covering the implementation of the SDO’s standards?
2. If so, must these participants agree to license such patents to all implementers of the standards?
3. If so, must these licenses be royalty-free, or may royalties be charged (and if so, are there any limitations on royalty-rates, F/RAND or otherwise)?
4. Must participants disclose these patents and, if so, when?

While at first blush it might appear that the above issues can be addressed in a relatively straightforward and concise manner, SDO antitrust and intellectual property policies have become increasingly complex and lengthy over the years. This trend can generally be attributed to the desire of SDO participants, and their legal counsel, to anticipate a growing range of legal contingencies and to accommodate the diverse interests and business models of those participants. For example, in a typical SDO that focuses on the development of next-generation wireless telephony standards, participants might include handset manufacturers, chip designers, service providers (carriers), software developers, and businesses that do no more than acquire and assert patents, not to mention academics, consumer advocates, and government agencies. It is not surprising that developing a policy that accommodates the requirements of each of these groups can be difficult, time-consuming, and expensive and can result in a complex policy that reflects myriad compromises required to appease these differing interests and business models.187

In contrast to the world of mobile telephony, participants in bioinformatics standards development activities currently appear to consist primarily of academics, industrial scientists, and a handful of product vendors. This observation, coupled with the general consensus around the simple intellectual property-related maxims described in Section VI.A above, suggests that bioinformatics SDOs might be able to adopt legally-prudent policies while avoiding the complexity, effort, and rancor often experienced in ICT-focused SDOs.

To this end, Appendix I contains a brief example of an SDO policy reflecting the two maxims noted above and other key provisions. While it is not intended that this exemplar be adopted verbatim by all bioinformatics SDOs, it is hoped that it might be useful as a starting point for consideration, and that it

---
might provide scaffolding atop which an SDO may build more specialized provisions to address the particularized needs of its participants.\textsuperscript{188}

C. Making Policies Binding

Even the most artfully-drafted SDO policy is of little value unless it binds its participants and possibly other implementers and users of its standards. Simply announcing the SDO’s policy on the SDO web site, without affirmative assent by those parties that the SDO intends to bind, will make the policy more difficult to enforce.\textsuperscript{189} Thus, SDOs have adopted a variety of approaches to ensure (or at least improve the chances) that their policies will legally bind their participants. These approaches include the incorporation of such policies into the SDO’s by-laws and other constitutional documents, the use of signed participation agreements, and the issuance of frequent reminders of the existence and effect of such policies.\textsuperscript{190}

Many bioinformatics standardization efforts are carried out in semi-academic settings without formal participation or membership structures. Groups of this nature would do well to consider formalizing their participation at least to the extent of requiring that participants expressly acknowledge (or, better still, agree to comply with) the SDO’s written policies.

VII. CONCLUSION

Though bioinformatics standards-development organizations have demonstrated a consistent preference for standards that are open and unencumbered by intellectual property rights, few of them have adopted explicit policies ensuring that these preferences will be respected by their participants. As evidenced by the increasing number of disputes and litigation in other fields that are heavily dependent on interoperability standards, it is important for organizations to adopt clear and binding policies governing the conduct of their participants. Accordingly, I recommend that bioinformatics standards-development organizations carefully review their existing policies and procedures. To the extent that they fail to address key points regarding process and intellectual property, I recommend that these policies and procedures be revised. In order to assist organizations with this exercise, I offer a straightforward policy template that is consistent with the observed norms and

\textsuperscript{188} The \textit{ABA Patent Policy Manual}, \textit{supra} note 178, contains a large collection of annotated sample clauses that appear in SDO patent policies. The exemplar presented in \textit{Appendix 1} is intentionally brief and does not delve into most of the complexities addressed by the Manual. For example, the exemplar policy does not address issues associated with the inclusion of software code in a standard, nor the licensing of patents on royalty-bearing terms.

\textsuperscript{189} See, e.g., Specht v. Netscape Commc’ns Corp., 306 F.3d 17 (2d Cir. 2002) (holding that a user of an online service is not deemed to have agreed to a vendor’s terms of service available when those terms were not conspicuous and the user was not required to assent to them explicitly).

\textsuperscript{190} See \textit{ABA Standards Manual}, \textit{supra} note 178, at 27.
goals of bioinformatics standards organizations. It is my hope that these modest prophylactic measures will enable the bioinformatics standards community to continue to work productively and avoid the disruptive and costly litigation that has affected other standards-dependent sectors.
APPENDIX 1

Sample Bioinformatics “Open” Standards Development Policy

[Insert name of standards development organization (SDO)] is committed to the open and transparent development and dissemination of technical standards relating to [subject matter]. Accordingly, all meetings, working groups, mailing lists, correspondence and other activities conducted under the auspices of SDO (“SDO Activities”) will be conducted in accordance with the following rules.

1. No Anticompetitive Conduct.

No SDO Participant\(^{191}\) shall, during or in connection with any SDO activity:
   a. discuss product prices, profits, internal cost, bidding, terms of bidding, allocation of customers, division of sales markets, sales territories, or marketing strategies;
   b. condition or discuss conditioning the implementation of an SDO standard on the implementer’s use of products or services offered by a particular party; or
   c. agree with others to refuse to do business with a particular party.

2. Copyright License.

   a. Each SDO Participant hereby grants to SDO and each other SDO Participant a non-exclusive, perpetual, royalty-free copyright license to reproduce, modify, distribute and create derivative works of every document, proposal, text, code, comment or other written item submitted by such SDO Participant to SDO or other SDO Participants in connection with any SDO Activity which is intended to influence or be incorporated into any draft or final standard (a “Contribution”). SDO Participants otherwise retain all rights in their respective Contributions.
   b. Each SDO Participant agrees that the copyright in any final standard published by SDO shall be owned by SDO, subject to SDO Participants’ ownership of their individual Contributions.


   a. Each SDO Participant agrees that it shall not, at any time during or after its participation in SDO, assert or seek to collect royalties on any patent that is necessary to implement an SDO standard (“Necessary Patent”) against any product or process that implements that SDO standard.

---

\(^{191}\) The term “SDO Participant” must be defined to include all members, organizers, promoters and other participants in SDO Activities.
b. Each SDO Participant shall ensure that the obligations in Paragraph 3.a bind the transferee of any Necessary Patent, and shall notify any actual or proposed transferee of any Necessary Patent of such obligations.

4. No Confidential Information.

No Contribution submitted by any Participant shall be deemed to be proprietary or confidential, and neither SDO nor any SDO Participant shall have any obligation to maintain any Contribution as confidential.
THE EMERGING CONFLICT BETWEEN NEWSWORTHINESS AND THE RIGHT TO BE FORGOTTEN

Jasmine E. McNealy, J.D., Ph.D.*

I. INTRODUCTION

In late 2010, Harvey Purtz filed a small claims lawsuit against Rajesh Srinivasan. The filing of a small claims suit would normally be insignificant, but Purtz’s reason for doing so makes the case interesting. Purtz claimed that Srinivasan had subjected him and his wife to intentional infliction of emotional distress by refusing to remove articles about Purtz’s son from the Daily Californian newspaper’s online archives.1 The newspaper articles, more than four years old at the time, detailed Chris Purtz’s drunken confrontation with the staff at a San Francisco strip club. Purtz was suspended from the UC Berkeley football team after the incident. He finally left the team in February 2007 for personal reasons,2 and died in June 2010.

A month after Chris’ death, Harvey Purtz contacted Srinivasan, the then editor-in-chief of the Daily Californian, and requested that the articles about his son be removed from the online archive. Srinivasan declined, citing company policy that content only be removed if it qualifies for a retraction.3 Purtz subsequently filed a lawsuit seeking $7,500 in damages. In his opinion ruling in favor of Srinivasan, the small claims judge noted that he was sympathetic to the pain Purtz had endured from the loss of his child.4 However, this gave Purtz neither the standing nor the basis for a claim against Srinivasan.5

The Purtz claim is interesting in that it appears to fly in the face of all traditional jurisprudence with respect to privacy and free expression. Although not specifically stating as much, Purtz was asserting a right to have information about his son, particularly negative information about his son, forgotten, erased from online archives. If allowed, an individual would be able to claim that the information about them contained in online newspaper archives was no longer

* Jasmine McNealy is an Assistant Professor at the S.I. Newhouse School of Publication Communication at Syracuse University. She earned a joint M.A./J.D. in 2006 and a Ph.D. in 2008 from the University of Florida. She also earned a B.S. in 2002 from the University of Wisconsin.

2. Id.
3. Id.
5. Id.
necessary, and should therefore be removed. Such a right would conflict with the tradition of allowing the public to have access to information, and for news organizations to publish information of a public concern, including arrests and court cases.

Such a right is not unfamiliar to a few of the countries in the European Union; some have used privacy-related legislation to allow an individual to stop unwanted retention of personal information. In 2009, for instance, a German man sent Wikipedia a cease and desist letter claiming that the online encyclopedia must remove information about him. The man, Wolfgang Werlè, who was tried and convicted of killing his former associate, Walter Sedlmayr, used a German law quite like American common law misappropriation, which protects an individual’s name and likeness from unwarranted publicity. In early 2010, France also began considering a “right to forget,” which would allow an individual to demand that online organizations delete information about them.

Although EU member states hail the creation of this right to be forgotten as improving individual privacy rights, such a right creates a problem for U.S. online news organizations. Not only does such law come into direct conflict with protections found in the First Amendment, but it also conflicts with traditional privacy jurisprudence, which states that information made public cannot become private again. At the same time, the *Purtz* case demonstrates that some plaintiffs in the U.S. seem to be attempting to assert a right to be forgotten.

This paper analyzes the emerging conflict that recognizing a right to be forgotten online would have with American jurisprudence regarding the role of the press, both traditional and online, as a watchdog for the public as well as with traditional U.S. privacy policy. Section II attempts to examine the boundaries of the right to be forgotten from both theoretical and EU perspectives. Section III considers traditional U.S privacy law and some of the contours of that law, including protections for newsworthy information. Section IV analyzes the right to be forgotten with respect to the protections for free expression detailed in Section III. This paper concludes with a consideration of how the right to be forgotten would not fit with traditional U.S. privacy jurisprudence.

II. THE RIGHT TO BE FORGOTTEN

The right to be forgotten is an idea based in a Westinian conception of privacy: that people and organizations should be permitted “to determine for

---


7. *Id.*

themselves when, how, and to what extent information about them is communicated to others."9 Yet, even with such a recognized foundation, what, exactly, the right to be forgotten entails has not been adequately defined. A few authors have arrived at similar but slightly different ideas of what the theory involves; the most general idea of which is the right to have certain information erased.

A. Defining the Right

According to Koops, the right to be forgotten takes three forms in the literature: the right to have information deleted after a certain time, the right to have a “clean slate,” and the right to be connected only to present information.10 The first conception of the right centers on the idea that individuals should have the opportunity to require other individuals and organizations in possession of information about them to erase it. The assertion of this right would arise when individuals upload information themselves, as well as when another person has placed information about the individual online.11 Difficulties arise with enforcement of such a right because multiple parties exist that might be in possession of the personal information, as well as the possibility that some possessors of information might be required to retain information under the law.12 To this end, some scholars have suggested that individuals should be able to set expiration dates for their information, thereby requiring that great consideration be given regarding what information can be made available for collection by others.13

The second and third theories of the right to be forgotten, the clean slate and the right to only be connected to current information, are similar. Both center on the idea that individuals can grow and change, and should not, therefore, be forever connected to information from the past that could be damaging. Analogous rights are provided in bankruptcy cases and the sealing of juvenile criminal records.14 In these cases, individuals, for the most part, do not have the specter of past ills or bad decisions available for others to use to judge them. The right to be forgotten would then allow people to “shape their own lives,” instead of having the memories of others do so for them.15 To this end, Murata and Orito offer this definition of the right: “An individual has the right to be free

11. Id. at 237.
12. Id. at 238–39.
14. Koops, supra note 9, at 250.
15. Id. at 251.
from any use of information concerning him/her which causes harmful effects on him/her. 16

This definition of the right to be forgotten, as well as others like it, places the right in conflict with other traditionally protected rights. In his conceptualization of “the right to delete,” Conley embraces a legal right of individuals to choose what information to retain or delete. 17 At the same time, he notes that such a right may come into conflict with competing interests like freedom of expression, contract, preservation of information, etc. With respect to freedom of expression, Conley offers a partial solution for limiting the right to delete to non-expressive content. 18 Further, Conley asserts that perhaps the right should include an exception for information deemed “newsworthy,” but notes that defining newsworthiness is difficult. 19 The difficulty in defining what the right to be forgotten entails, as well as the creation of exceptions for this right, make defining its boundaries problematic. It might, therefore, be instructive to examine how one government is implementing this right.

B. The European Perspective

In October 2010, the European Commission began circulating a draft strategy aimed at improving data protection. 20 The proposal noted that changes in technology necessitated a revamped strategy and improvement to the EU Data Protection Directive. According to Zwick and Dholakia, the 1995 European Union Privacy Directive makes an individual the “inalienable possessor of his or her own personal data.” 21 The Directive broadly defines personal data, and requires that those in possession of personal data meet certain obligations intended to prevent the misuse of such data. 22

The draft proposal includes strategies for standardizing privacy notices, strengthening consent rules, and new rules for what constitutes sensitive data. Also included in the draft proposal was the creation of a “right to be forgotten.” This right to be forgotten would give individuals the right to not have their data retained and expressly deleted when the data is no longer needed for a legitimate purpose. Under the draft strategy, a data subject, or the person who may assert the right, is defined as any identified person or person who could be identified using “reference to an identification number, location data, online identifier or to

---

18. Id. at 56.
19. Id. at 256.
22. Id.
one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.” Personal data, then, is any information by which a data subject could be identified. This definition of personal data is quite broad, and could reasonably include any information collected by journalists.

The right to be forgotten is a right to erasure of information in the possession of other parties. Under the proposed Article 17, individuals could assert this right in situations where they no longer consent to a second party using their information. The General Data Protection Regulation provides four grounds for allowing a data subject to seek the erasure of information: (1) the information is no longer necessary for the purposes for which it was originally collected, (2) the data subject no longer consents to the retention of the information or the consent has expired, (3) the data subject objects to the processing of the information, and (4) the processing of the data does not comply with other sections of the Regulation. In compliance with the Regulation, the controller must erase the personal data immediately.

There are, however, exceptions to forced erasure, including an exemption for personal data that is necessary for “exercising the right to freedom of expression.” Article 80 of the Regulation requires EU countries to create such exemptions for journalistic purposes, and to report said exemptions to the EU Commission on Human Rights immediately. What such exemptions for freedom of expression will look like remains to be seen. Werro, in his 2009 work examining the right to be forgotten, hypothesized that in the conflict between the right to be forgotten and press freedom, a European court would rule that privacy outweighed freedom of expression in certain instances. Werro arrived at this conclusion after an examination of Swiss legal cases, in which Swiss courts ruled that an individual’s right to rehabilitate his name trumped the right of the press to report on that individual’s criminal record.

To examine how exactly an EU member state would enforce the right to be forgotten, it might be useful to consider Spain’s recent assertion of the right against Google. Mario Gianni Masiá, the owner of Los Alfaques campground in

24.  *Id.* at 41.
27.  *Id.*
28.  *Id.*
29.  *Id.* at 52.
30.  *Id.* at 94-95.
32.  *Id.* at 290-91.
Spain, recently sued Google’s Spanish subsidiary in local court. Masiá sued over Google search results for the campground that led to news information, photos, and a Wikipedia page detailing a more than 30-year old disaster there, in which more than 200 people were burned to death. Spain allows its citizens to sue to force companies to erase information held about them under the Spanish Data Protection Authority. Masiá lost his case because he failed to sue Google directly. For its part, the Audiencia Nacional, Spain’s highest court, sent a request to the European Court of Justice (ECJ) inquiring whether EU citizens can demand that Google delete information about them. The ECJ’s answer should prove instructive as to the boundaries of the right to be forgotten, especially with respect to search engines like Google, whose search results include news articles. It might also indicate how the EU will apply the right to organizations, like Google, which are headquartered in countries with more exemptions for information dissemination vis-à-vis invasion of privacy.

III. PRIVACY IN THE U.S.

The bedrock of tortious invasion of privacy in the United States is an 1890 Harvard Law Review article by future U.S. Supreme Court Justice Louis Brandeis and Samuel Warren. The Right to Privacy, as the article was entitled, called for the recognition of a “right to be let alone.” Some say that this article was motivated by harassment, as an East Coast press corps went so far as to crash the wedding reception that one of the authors held for his daughter. Whatever the case may be, Warren and Brandeis conceptualized a new tort, akin to defamation; but instead of punishing false information, this tort would allow an injured party to recover for the disclosure of truthful information that was unprivileged and non-public. Of particular interest to Warren and Brandeis was

35. Anderson, supra note 33.
36. Id. at 31.
39. 4 Harv. L. Rev. 193 (1890) (Warren and Brandeis were not the first to ponder the right to be let alone. The authors recognize Judge Thomas Cooley as having written about it previously); Id. (citing Thomas C. Cooley, Law of Torts, 29 (2d ed. 1888)).
the ability of a person to be free from harassment, especially by the press who had “overstepp[ed] in every direction the obvious bounds of propriety and decency,” filling their pages with “idle gossip.”

Legislatures and courts began recognizing privacy torts soon after the article’s publication.

Although Warren and Brandeis’s article was innovative, it was not until seventy years later, with the publication of another law review article that the idea of a common law right to privacy took hold. In his 1960 California Law Review article, Dean Prosser fleshed out the idea of an invasion of privacy tort, dividing it into four separate causes of action. In evaluating the privacy cases that had arisen after Warren and Brandeis published their article, Prosser found that “[t]he law of privacy comprises four distinct kinds of invasion of four different interests of the plaintiff . . . .” These causes of action include appropriation, intrusion, false light and public disclosure, the action most similar to that thought of by Warren and Brandeis. It is important to note that Prosser theorized divisions in a privacy tort, because he later authored the invasion of privacy section in the Restatement of Torts. This section, detailing common law actions for privacy invasions, was subsequently followed by many state courts, and used as model law for many state legislatures.

The Restatement, in sum, defines the tort for publication of private facts as the publication of private truthful information about an individual that is highly offensive to a reasonable person. Like many torts that deal with punishing speech, it would seem that this tort might offend the First Amendment. There have been successful prosecutions for public disclosure of private facts, especially for disclosure of illnesses or hospitalization information; one such case was Barber v. Time, Inc. In Barber, a woman suffered from a disease that made her lose weight in spite of the amount of food she consumed. A reporter from Time entered her hospital room, and in spite of her protests, took her picture. The magazine ran the picture in an article calling Ms. Barber the “Starving Glutton.” The Missouri state courts found for the plaintiff in this case, and held the newspaper liable for invading the woman’s privacy.

Public disclosure of private facts uses a reasonableness expectation, asking whether a defendant’s publication of private information about the plaintiff was highly offensive to a reasonable person. This highly offensive requirement

40. Id. at 196.
43. Id. at 389.
44. Rest. (2d) Tort § 652D.
45. 159 SW.2d 291 (Mo. 1942).
46. Id. at 293.
47. Id. at 296.
48. Id. at 292.
49. Id. at 296.
50. Rest. (2d) Tort § 652D at comment (c).
weighs societal views of offensiveness. It is, for example, highly offensive to a reasonable person to publish a photograph of a woman whose dress has accidentally blown up above her head in public,\(^\text{51}\) or to report that someone suffers from a rare disease.\(^\text{52}\) At the same time it is not highly offensive to publish a picture of a young couple kissing at a restaurant,\(^\text{53}\) or of a young woman exposing her breasts at a rock concert.\(^\text{54}\)

A. Newsworthiness

In addition, the law of public disclosure of private facts precludes recovery where the published private information is not of “legitimate public concern.”\(^\text{55}\) However, the Restatement offers that the publication is subject to First Amendment protection if the defendant can show that the information is of public concern.\(^\text{56}\) Although “of public concern” would obviously anticipate news, it also includes entertainment, film, books, and most anything that stops short of a morbid fascination.\(^\text{57}\)

Although the U.S. Supreme Court has yet to make any definitive statement about the limits of newsworthiness with respect to personal privacy, the lower federal and state courts have developed a few tests that set boundaries on free speech, especially with respect to the tort of invasion of privacy by public disclosure of private facts. Geoff Dendy, in his 1997 Kentucky Law Review student article, noted four different approaches to newsworthiness.\(^\text{58}\) In a San Diego Law Review student article published two years later, John Jurata identified five different approaches to newsworthiness.\(^\text{59}\) The discrepancy in the number of approaches enumerated by Dendy and Jurata can be explained by the fact that Dendy theorizes that two of the approaches are so similar as to be thought of as only one approach. This paper considers Jurata’s approach.

First, Jurata recognized the Restatement’s approach to newsworthiness, which privileges the publication of information that is of public concern, is not highly offensive to a reasonable person, and stops short of a morbid fascination.\(^\text{60}\) An example of this is Virgil v. Time, in which a then-famous surfer sued Sports Illustrated for public disclosure of private facts.\(^\text{61}\) A Sports

\(^{51}\) See Daily Times Democrat v. Graham, 162 So. 2d 474 ( Ala. 1964).

\(^{52}\) See Barber v. Time, Inc., 159 S.W.2d 291 (Mo. 1942).


\(^{55}\) Rest. (2d) Tort § at comment (h).

\(^{56}\) Id.

\(^{57}\) Id.


\(^{60}\) Id. at 496.

Illustrated reporter wrote an article detailing Virgil’s weird habits of using his mouth to put out cigarettes, drug use, and diving down flights of stairs to impress women.62 The court ruled that the details of Virgil’s life were sufficiently newsworthy.63 Because the Restatement approach places particular emphasis on community standards,64 it is suspected that most of these cases would be decided by a jury, and not by summary judgment.

A second approach to newsworthiness involves rejection of the publication of private facts tort outright.65 States may reject publication of private facts through judicial opinion or by statutory creation of the state legislature, thereby expressly exempting publication of private facts as a viable action. However, even though this approach is an option, it is not adopted by many jurisdictions. Yet, in those jurisdictions that have rejected publication of private facts as a cause of action, it is implied that every publication of truthful information is newsworthy.66 This explicitly gives the First Amendment priority over personal privacy.67

A third approach is the “leave-it-to-the-press-model.”68 This test for newsworthiness expresses courts’ unwillingness to meddle in the editorial process of the press. So named by Professor Diane Zimmerman in her 1983 Cornell Law Review article, “Requiem for a Heavyweight: A Farewell to Warren and Brandeis’s Privacy Tort,”69 this approach reflects courts’ hesitance to question what is considered news fit to print, especially after Miami Herald v. Tornillo.70 Although the case did not involve publication of private facts, in Tornillo the U.S. Supreme Court decided that it was not the province of a court to decide what a newspaper must print.

A fourth approach, which I will call the California approach, is similar to that of the Restatement. This test for newsworthiness, as created by the California Supreme Court uses the Restatement conception of newsworthiness, but has an added prong that deals with the intent of the publisher.71 The California courts do not recognize newsworthiness as a defense to a publication of private facts claim if the publisher is found to have published the information recklessly.72 The California test was first delineated in Kapellas v. Koffman, in which the adult children of a candidate for public office claimed that they were injured, under a theory of publication of private facts, when news was published.

62. Id. at 1289.
63. Id. at 1290.
64. Rest. (2d) Tort § 652D at comment (h).
65. Jurata, supra note 59, at 503.
66. Id. at 504.
67. Id.
68. Id. at 505.
71. Jurata, supra note 59, at 506.
72. Id.
about their juvenile criminal records. The court in Kapellas found for the publisher because the information was not published recklessly.

The last approach to newsworthiness is the logical nexus test. According to Jurata, the logical nexus test is used mostly by the U.S. Courts of Appeals for the Tenth and Fifth Circuits, and is steadily gaining popularity. This test considers information newsworthy if that information has a logical relationship to an issue of public concern. This approach was most famously used in Campbell v. Seabury Press, in which the former sister-in-law of a civil rights leader sued a publisher over a book that detailed embarrassing information about her first marriage. Campbell lost her case because the Fifth Circuit determined that the information published about her first marriage formed a logical nexus with the life of the civil rights leader, the issue of public concern. Critics of this approach say that it sweeps too broadly, as most people are involved in some activity of public concern. Therefore, this test would seemingly allow no recovery for publication of private facts.

All of these approaches seem to offer great First Amendment protection for the publication of truthful, yet private, information. Although the approaches differ, one can see how application of each of the different tests might produce the same result using, for example, the Virgil case. Under the Restatement and California approaches, a court would look at whether the information goes beyond the bounds of good taste to morbid fascination. The approaches would also look to the standards of the community to decide the case. The court found that the information published about Virgil was newsworthy because it dealt with the antics of someone in the public. The California approach would also force the court to decide whether the information was published recklessly; in this case, the court could find that there was no recklessness because Virgil knew he was being reported on by journalists and still engaged in his behavior. In those jurisdictions that reject publication of private facts, Virgil would not have a claim against the press at all. In a jurisdiction following the leave-it-to-the-press approach Virgil would also, mostly likely, not succeed in his claim for invasion of privacy because the courts would not question the editorial judgment of Sports Illustrated to publish the information. Finally, the courts could find a logical nexus between a matter of public interest, or Virgil’s status as a star surfer, and the information printed about Virgil’s drug use, stair diving, and cigarette eating.

Further, the public interest in certain information does not necessarily degrade over time. This is perhaps the concept in American privacy law that is most at odds with a right to be forgotten. The classic case for this is Sidis v. F-R

74. Jurata, supra note 59, at 507.
75. ld.
76. 614 F.2d 395 (5th Cir. 1980).
77. Jurata, supra note 59, at 508.
Publishing Corp. in which the U.S. Court of Appeals for the Second Circuit ruled that a man who had received great media attention for his intellect as a child was still considered newsworthy over twenty years later. Similarly, an allegedly abusive ex-husband who had since reformed was deemed newsworthy, even after a significant lapse of time. Plaintiffs have only been awarded damages for invasion of privacy in very few cases based on information published long after the events took place. In *Melvin v. Reid*, for example, a former prostitute, who had been tried and acquitted of murder, sued a filmmaker who made a film based on her life. The California appellate court awarded damages to Gabrielle Darley, who by that time had married and turned away from her former life, based on the filmmaker’s infringement, not of Gabrielle’s right to privacy, but of the right “to pursue and obtain safety and happiness.” The California court refused, however, to recognize a property right in Darley’s name and the facts about her life.

**B. Statutory Privacy and the First Amendment**

Although public disclosure of private facts is a common law privacy tort that has been codified by the majority of the states, there exist other similar statutory privacy actions individuals may assert. Like public disclosure, these statutory claims have run into conflict with freedom of speech. A line of U.S. Supreme Court cases deals specifically with this conflict. One of the first Supreme Court decisions in this line of cases was *Cox Broadcasting Corp. v. Cohn*. In *Cox Broadcasting*, the father of a teenage rape and murder victim sued the owner of a news station after a reporter broadcast the name of the victim. A Georgia statute made it illegal to publish the name of a rape victim, and the father claimed that Cox had invaded his privacy under the Georgia statute by broadcasting his daughter’s name during a news segment.

The Court ruled that the Georgia statute directly conflicted with the First Amendment. The majority focused on the narrow issue of whether a state can punish the publication of the name of a rape victim if the name is obtained from public records. The Court decided that the state could not punish the

---

78. 113 F. 2d 806 (2d Cir. 1940).
81. *Id.* at 93.
82. *Id.* at 93-94.
84. *Id.* at 474.
85. *Id.* The Georgia statute made it “unlawful for any news media or any other person to print and publish, broadcast, televise or disseminate through any other medium of public dissemination or cause to be printed...in this State or though any radio or television broadcast originating in the State the name or identity of any female who may have been raped or upon whom an assault with intent to commit rape may have been made.” *Id.* at 471 (citing GA. CODE ANN. § 26-9901 (1972)).
86. 420 U.S. at 489.
87. *Id.* at 491.
publication, and found that the press has a responsibility to report on the actions of government, including judicial proceedings and information that is part of the public record. The Court further held that the Georgia statute sanctioned pure expression and not a combination of speech and action. The justices declined, however, to decide the larger question of whether publication of truthful information could ever be punished.

The Court’s decision in Oklahoma Publishing Co. v. District Court for Oklahoma County picked up where Cox Broadcasting left off. In Oklahoma Publishing, reporters attended a detention hearing and learned the name of a boy accused of fatally shooting a railroad switchman. One reporter took a picture of the boy as he was taken from the courthouse. Later, at a closed arraignment, the judge entered a pretrial order enjoining publication of the boy’s name and picture. The journalists’ motion to quash the order was denied.

The U.S. Supreme Court reversed the trial judge’s decision and based its ruling on Cox Broadcasting and Nebraska Press Association v. Stuart, which, according to the Court, reaffirmed Cox Broadcasting: “the press may not be prohibited from ‘truthfully publishing information released to the public in official court records.’” The Court cited the fact that the juvenile hearing, whether actually closed by the judge or not, was actually attended by the journalists with the judge’s knowledge. There was, therefore, no evidence that the reporters acquired the information unlawfully or without approval.

The issue of acquiring and publishing information from closed hearings resurfaced a year later in Landmark Communications, Inc. v. Virginia. The Commonwealth of Virginia had a law which made proceedings and documents of its Judicial Inquiry and Review Commission confidential. Any disclosure of the information from the proceedings was considered a misdemeanor.

88. Id. at 496.
89. Id. at 492. “Without the information provided by the press most of us and many of our representatives would be unable to vote intelligently or to register opinions on the administration of government generally. With respect to judicial proceedings in particular, the function of the press serves to guarantee the fairness of trials and to bring to bear the beneficial effects of public scrutiny upon the administration of justice.” Id.
90. Id. at 495.
91. Id. at 491.
93. Id at 309.
94. Id.
95. Id.
96. 427 U.S. 539 (1976) (holding that a court order prohibiting the publication, by the press, of certain trial information unconstitutional).
97. Oklahoma Pub’g, 430 U.S. 310 (quoting Cox, 420 U.S. at 496).
98. 430 U.S. at 311.
99. Id.
101. Id. at 830 (citing VA. CONST. ART. 6 § 10; VA. CODE § 2.1-37.13 (1973)).
102. Id. “Any person who shall divulge information in violation of the provisions of this section shall be guilty of a misdemeanor.”
In 1975, the *Virginia Pilot*, a newspaper published by Landmark Communications, published an article identifying a judge involved in a then pending Commission investigation.\(^{103}\) The newspaper was indicted and found guilty of violating the Virginia statute.\(^{104}\) The U.S. Supreme Court reversed the conviction, finding the statute unconstitutional as applied to Landmark and the press.\(^{105}\) As it had ruled in *Cox Broadcasting*, the Court found that court proceedings and the conduct of judges were matters of public concern.\(^{106}\)

In *Landmark*, the Court again expressly declined to answer the question of whether the truthful publication of information could ever be punished.\(^{107}\) Instead, the Court decided to answer the narrow question of whether a third party could be punished for publishing confidential information concerning proceedings of the Judicial Commission.\(^{108}\) Further the Court stated that it was not concerned, in this instance, with the individual who “secures the information by illegal means and thereafter divulges it.”\(^{109}\) The Court concluded that the speech that the statute sought to suppress was at the very core of First Amendment protection.\(^{110}\)

*Smith v. Daily Mail Publishing Co.*,\(^{111}\) decided a year after *Landmark*, synthesized *Cox Broadcasting*, *Oklahoma Publishing*, and *Landmark*, and ruled that the cases “suggest strongly that if a newspaper lawfully obtains truthful information about a matter of public significance then state officials may not constitutionally punish publication of the information, absent a need to further a state interest of the highest order.”\(^{112}\) *Daily Mail* involved facts similar to both *Landmark* and *Oklahoma Publishing*. West Virginia had a statute criminalizing the publication of the name of a juvenile in connection with judicial proceedings, without a written order from the court.\(^{113}\) Reporters for *The Daily Mail* newspaper printed the name of a juvenile murder suspect\(^{114}\) after interviewing witnesses to a junior high school shooting, which the reporters learned of while listening to a police scanner.\(^{115}\)

---

103. Landmark Commc’ns Inc. v. Virginia, 435 U.S. at 831.
104. Id. (see Landmark Comm. Inc. v. Virginia, 233 S.E.2d 120, 122 (Va. 1977)).
105. Landmark, 435 U.S. at 838.
106. Id. at 839.
107. Id. at 840.
108. Id. at 837.
109. Id. The Court stated that there was not a constitutional challenge to Virginia’s power to keep Commission proceedings confidential or to punish Commission participants for breaching that confidentiality.
110. Id at 838.
112. Id. at 103.
113. Id. at 108-09 (citing W. Va. Code § 49-7-3 (1976)).
114. Daily Mail, 443 U.S. at 99-100. The newspaper printed the name a day after another newspaper and three radio stations published the juvenile’s name.
115. Id. at 99.
A grand jury indicted *The Daily Mail* for knowingly violating the state statute.\textsuperscript{116} Affirming the decision of the West Virginia Supreme Court, the U.S. Supreme Court held that the indictment was an unconstitutional prior restraint.\textsuperscript{117} The Court emphasized that its holding was narrow.\textsuperscript{118} It defined the issue as whether a state had the power to punish the “truthful publication of an alleged juvenile delinquent’s name lawfully obtained by a newspaper.”\textsuperscript{119} In doing so, the Court again avoided the question of whether the truthful publication of information could ever be punished.\textsuperscript{120}

*Florida Star v. B.J.F.*\textsuperscript{121} involved a statutory prohibition on printing the name of a sexual assault victim.\textsuperscript{122} *The Florida Star* newspaper printed a police brief describing a reported sexual assault and using the assault victim’s name.\textsuperscript{123} A reporter-trainee obtained the information for the brief by copying a police report, which had been made available in the police department’s pressroom.\textsuperscript{124} In reversing B.J.F.’s jury award, the Court found that the name of the rape victim was lawfully obtained and that information was publicly available.\textsuperscript{125} The Court particularly noted that one of the important reservations it had with the Florida statute was that it was “facially underinclusive.”\textsuperscript{126} Instead of prohibiting anyone to disclose the sexual assault victim’s name, the statute actually limited the prohibition to “instrument[s] of mass communication.”\textsuperscript{127} As such, an individual disclosing the name of a rape victim would not be punished. The Court concluded that, “[w]hen a State attempts the extraordinary measure of punishing truthful publication in the name of privacy, it must demonstrate its commitment to advancing this interest by applying its prohibition evenhandedly, to the smalltime disseminator as well as the media giant.”\textsuperscript{128}

These cases demonstrate that even when privacy is protected by statute, the individual bringing the claim has to demonstrate a high level interest before a court will enforce a sanction against the press. The use of strict scrutiny in statutory privacy cases creates an almost impossible hurdle for plaintiffs to overcome. This line of cases establishes that the publication of truthful, lawfully

\begin{itemize}
\item \textsuperscript{116} Daily Mail Publ’g Co. v. Smith, 248 S.E.2d 269, 270 (W.Va. 1978) (The newspaper filed for and received a writ of prohibition from the West Virginia Supreme Court).
\item \textsuperscript{117} Daily Mail, 443 U.S. at 106.
\item \textsuperscript{118} Id. at 105.
\item \textsuperscript{119} Id. at 105-06.
\item \textsuperscript{120} Id. at 105. “There is no issue before us of unlawful press access to confidential judicial proceedings.”
\item \textsuperscript{121} 491 U.S. 524 (1989).
\item \textsuperscript{122} Id. at 526. The Florida statute made it unlawful to “print, publish, or broadcast in any instrument of mass communication…the name…of the victim of any sexual offense. Fla. Stat. § 794.03 (1987).
\item \textsuperscript{123} Florida Star, 491 U.S. at 527.
\item \textsuperscript{124} Id.
\item \textsuperscript{125} Id. at 536-39.
\item \textsuperscript{126} Id. at 540.
\item \textsuperscript{127} Id. (The statute did not define “instrument of mass communication”).
\item \textsuperscript{128} Id.
\end{itemize}
acquired information receives a high level of First Amendment protection. It remains to be seen whether the same standard would be used in cases dealing with the right to be forgotten.

IV. ANALYZING THE CONFLICT

It is important to reiterate that no such right to be forgotten exists in the U.S. Yet, the Purtz case and other much older cases demonstrate that individuals have asserted, and continue to assert, claims of a similar right. It may be instructive, then, to consider Purtz from a right to be forgotten perspective. Within this perspective, it is also necessary to hypothesize how U.S. courts would apply the exception for newsworthiness, as well as the strict scrutiny test, and what might be the outcome of these restraints on privacy.

First, it is necessary to review the facts of Purtz. The father of a former college athlete asked the editor of a college newspaper to remove articles about his son from the newspaper’s online archive. The editor refused to remove the articles, citing company policy not to do so unless a retraction was necessary. The father sued in small claims court alleging that the articles exposed him and his wife to emotional distress and should, therefore, be removed from the online news archive.

If Purtz could assert a right to be forgotten, he could claim that the articles about his son were no longer necessary because a significant amount of time had passed and the information was no longer being used for the purpose for which it was originally collected. In this case, that original collection purpose was to report on Chris Purtz’s trouble at the strip club, his suspension, and subsequent departure from the football team. The father could also claim that he was a data subject, because his social or cultural identity as the father of Chris Purtz could be recognized in relation to the articles about his son. As the data subject, he would have the right to request that the Daily Californian take the articles down, because the information about his son could lead to his identification.

If Purtz were to be able to assert the right to be forgotten he would face a major hurdle in the freedom of expression exception as expressed in the protection for newsworthiness. Because Purtz filed his claim in California, the California test for newsworthiness would be the most logical test to consider. Under this test, the court would privilege the publication of

130. Reimold, supra note 1
131. Id.
132. See definition of “data subject” supra note 23 and accompanying text.
information that is of a public concern, which is not highly offensive to a reasonable person, which stops short of a morbid fascination, and which was not published with reckless intent. The newspaper’s archived articles would pass all four prongs of this newsworthiness test. First, the articles focused on Chris’s troubles while he was a player on the football team of the school with which the newspaper was connected. In the California case that first detailed the state’s test for newsworthiness, even information about the juvenile arrest record of a public office candidate’s children was considered to be of a public concern. Information about the possibly criminal acts of a college athlete would certainly be considered information of interest to the public.

The articles would also not be highly offensive to a reasonable person because they reported on public events: Chris’ altercation at the strip club and his suspension from the team. Further, the reporting of public happenings could hardly be considered prying into the Purtzes’ private lives. Such information does not rise to the level of reporting on someone’s rare disease, which was ruled highly offensive in Barber. Finally, there was no evidence that the newspaper published the information recklessly. Therefore, Purtz would again fail in his claim against the newspaper if alleging a right to be forgotten. It is also important to note that Purtz would probably argue that the passage of time should diminish the newsworthiness of the information about his son. Yet, the courts have, for the most part, ruled that newsworthiness does not necessarily wane after time passes. This would certainly defeat the main rationale for asserting the right to be forgotten—that the information is no longer being used for the purposes for which it was originally collected.

As a second matter, Purtz would not be able to prove that the state had a high level interest in enforcing the right to be forgotten against the newspaper. The right to be forgotten, like the statutes and court orders in Cox Broadcasting, Oklahoma Publishing, Landmark, Daily Mail, and Florida Star, focuses squarely on protected expression. It would stand to reason that if the protection of the name of juveniles and rape victims did not trump the right to freedom of expression, it would be difficult for Purtz to prove that the right to be forgotten should do so.

V. CONCLUSION

The right to be forgotten is an emerging privacy-related tool for plaintiffs in order to have information about them removed from retention by organizations and availability online. The boundaries of the right to be forgotten have yet to be concretely defined, but draft legislation from the EU provides some guidance.
as to how such a right would be codified. The law would allow an individual, claiming to be able to be identified by certain information, to demand that an organization remove that information immediately. The organization would have to comply or face possible court ordered sanctions.

Built into this right is the protection for freedom of expression. Such an exception appears, however, analogous to the protection for newsworthiness built into the law of public disclosure of private facts invasion of privacy. Under the newsworthiness exception, the publication of information would be protected so long as that information was of a public concern, was not highly offensive to a reasonable person, was not morbid or prying, and was not published with recklessness. The Purtz case demonstrates that conflict between the emerging right to be forgotten and the right to freedom of expression as protected under the guise of newsworthiness. When Purtz is considered under the right to be forgotten, with the exception for newsworthiness, the case against the newspaper editor still fails.

How the countries of the EU will apply this exception to the right is not fully understood. The decision of the ECJ with respect to Spain’s question as to whether its citizens could demand that Google delete information about them under the right to be forgotten should prove instructive as to the reach of the right. Google search results certainly include links to news articles that could identify individuals. It remains to be seen whether the EU exception for freedom of expression within the right to be forgotten will protect access to the information in those articles.
DIGITAL DIVISIONS: RACIAL (IN)JUSTICE AND THE LIMITS OF SOCIAL INFORMATICS IN THE STATE OF GEORGIA VS. TROY ANTHONY DAVIS

Mark Lawrence McPhail*
Rachel Lyon **
David Harris ***

The recent decision by the Georgia State Board of Pardons to execute Troy Anthony Davis for the murder of police officer Mark McPhail raises a number of legal, social, and media issues that coalesce around questions of racial justice and reconciliation. The legal issues raised by the decision range from the unequal application of the death penalty to tensions between the rule of law and the rule of justice, between efficiency and fairness. The social issues cover terrains as diverse as the efficacy of new and traditional media coverage and advocacy, all democratic possibilities of social informatics, and raise fundamental questions about the value and validity of rational discourse in the justice system when race is a central issue. In this essay we will focus an interdisciplinary lens on the procedural, philosophical, and pragmatic tensions raised by the trial, media coverage, and eventual execution of Troy Davis. We seek to illuminate the ways in which legal, social, and moral attitudes and institutions remain tainted by the hidden racialized communication of the media.

* Mark Lawrence McPhail is Dean of the College of Arts and Communication at the University of Wisconsin-Whitewater. He is the author of Zen in the Art of Rhetoric: An Inquiry into Coherence, and The Rhetoric of Racism Revisited: Reparations or Separation? His research and creative work have appeared in The Quarterly Journal of Speech, Rhetoric and Public Affairs, the Howard Journal of Communications, Critical Studies in Mass Communication, Rhetoric Review, and Qualitative Inquiry. He has served as an expert witness in the state of Utah, and for the United National International Criminal Tribunal for Rwanda (UNICTR).

** Rachel Lyon is the Chair and Professor of Electronic Media and Broadcasting in the Department of Communication at Northern Kentucky University. She is an Emmy-Award-winning documentary filmmaker whose recent productions include Discovering the Etruscans: From the Temple and the Tomb, and Juror Number Six, an international Internet documentary with the Ford Foundation's blackpublicmedia.org's Masculinity Project, that was recently featured in the AFI Dallas Film Festival. Lyon's documentaries include the acclaimed, Race to Execution for PBS's Independent Lens, Mr. Dreyfuss Goes to Washington for The History Channel, Shadow Over Tibet for PBS and the Emmy Award winner, Men Who Molest, for PBS's Frontline. Special thanks to Victoria Mullins

*** David J. Harris is the Managing Director of the Charles Hamilton Houston Institute for Race and Justice at Harvard Law School. David has extensive experience in many facets of civil rights issues from police brutality and racial profiling, to redistricting and domestic violence, as well as fair housing and community development. He previously served with the U.S. Department of Housing and Urban Development (HUD) and with the U.S. Commission on Civil Rights, and presently serves as the President of the Board of Directors of the Massachusetts Foundation for the Humanities. He is recognized as a leading voice for civil rights in the Boston region and has spoken extensively at local, regional and national forums on civil rights, regional equity and fair housing.
Drawing upon critical theories of law, media, and race, we will challenge two prevailing social mythologies, one traditional and the other emergent: that an adversarial and retributive legal system can achieve racial justice, and that the decentralization of communication brought about by internet technologies alone can create and cultivate a more democratic public sphere. Central to our analysis is a critique of assumptions that rational-critical discourse can cultivate and sustain systems of social and legal relations that serve the public good. Instead, we argue that the legal and mediated communication structures in question remain wedded to what Charles Mills describes as a “Racial Contract,” an empirical set of social relations that expose law as a system of privilege that protects the interests of the stronger, and undermines genuine democratic inclusion, social equality, and racial reconciliation.

I. INTRODUCTION

On September 21, 2011, after serving more than twenty years on death row, Troy Anthony Davis was executed by the state of Georgia. The Davis case garnered international attention from death penalty opponents around the globe, and received substantial attention from traditional and new media. Despite this attention, after “weighing all the facts,” the Georgia State Board of Pardons denied Davis’s final appeal for clemency.1 The Davis case raises several important issues: the role of race in the criminal justice system; the effectiveness of legal safeguards to protect against wrongful executions in death penalty cases; and the limits of social and traditional media to influence public attitudes, debate, and policy. The case also sheds light on the historical and cultural constraints and limitations of a legal system based upon retributive justice, and offers insights into how alternative approaches to crime and punishment might more productively guarantee the rights and liberties of all members of society.

This essay will explore these questions vis-à-vis critical perspectives on law, race, and media, and then consider what these analytical approaches can tell us about the past, present, and future of our system of jurisprudence as it relates to race, retribution, and reconciliation. The essay will begin by placing the case within a contemporary context and examining the conversations and debates it initiated in the public sphere. Next, it will offer a critical interrogation of the case that integrates the insights of critical legal, race, and media scholarship in exploring intersections between the cultural, institutional, and attitudinal impulses that framed those events and conversations. Finally, the essay will

---

examine what the case might mean for how justice is conceived and enacted, and how issues of crime and punishment might alternately be addressed in this society.

The purpose is not to consider the innocence or guilt of the individual, Troy Davis, but to consider more broadly how innocence and guilt function in a society informed by what philosopher Charles Mills calls “The Racial Contract.” Mills contends that the legal and political institutions of Western societies, built upon the foundations of contractarian ideals, have failed to enact those ideals because of their collective and possessive investments in “whiteness.” This failure has its roots in the tension between the democratic and egalitarian impulses of Western moral philosophy, and the history of European colonialism and imperialism that arose simultaneously with those impulses. The result has been an irreconcilable conflict between principle and practice that undermines the emancipative projects of Western law and politics.

The Davis case is but one of many examples of that conflict, yet it offers the opportunity to explore new ways of making meaning of the schism between an idealized social contract and the reality of the Racial Contract. It also enables us to consider the problems and possibilities presented by technology for the creation of an inclusive and egalitarian polity. While race was arguably one of the central issues in the case, its significance might best be understood through an examination of the epistemological, ideological, and institutional forces that have, and continue to, shape its meaning in American law and society. This is the purpose of this analysis which, the authors believe, holds important implications for critical legal, race, and media scholars and practitioners committed to enacting theoretical and practical strategies that facilitate political, economic, and social justice.

II. THE TRIALS OF TROY ANTHONY DAVIS

*State of Georgia v. Troy Anthony Davis* is a case that is an all too familiar story in our collective social narrative about race, media, and justice. A black man is accused of murdering a white policeman in the South. He is depicted in the media as a monster: accounts of the trial published in the newspaper report that witnesses testify that he “smiled” over the body of the wounded policeman as he delivered the fatal shot. He is reported to have “bragged and boasted” about the shooting, is implicated in another shooting earlier that night, and was involved in the beating of a homeless man when the murdered officer arrived at

3. The State of Georgia v. Troy Anthony Davis, EF 284361, Criminal Indictment Number 089-2467-H, Superior Court of Chatham County, State of Georgia.
the scene.\(^5\) He is reported to have fled the scene, and turned himself in after a “relentless” five-day manhunt, claiming that he was innocent of the crime.\(^6\) News outlets document his trial, conviction, and sentencing to execution by a jury of his peers, and as he begins the journey of a death row inmate, fighting for his life through an appeals process that is expensive and slow, the trial fades from public view.

Several years later, however, a new story emerged, still familiar, but far less black and white. Stories of witness recantations, evidence of police coercion, and a new theory of the crime. All of these thrust the case back into the media spotlight, and drew the attention of people from across the nation, as well as celebrities, advocates of racial equality and social justice, and proponents and opponents of the death penalty from around the globe.\(^7\) The case was also framed by an emerging set of issues and concerns related to race and fairness in the justice system. DNA testing revealed that large numbers of innocent black men had been convicted on the basis of inaccurate witness testimony;\(^8\) rising incarceration rates for African American men raised questions about the use of the penal system as a form of modern disenfranchisement and enslavement;\(^9\) and media critics and legal scholars were increasingly concerned about the influences of representations of crime and criminality in news and popular media.\(^10\)

The story of the trial also found a new technological venue for expression: the Internet and World Wide Web. More voices than ever before were joining conversations about race, crime, and social justice, and the diversity of voices ranged from experts to ordinary people. This enlarged public sphere of discourse was by no means unproblematic: just as supporters of Davis could

---

7. AMNESTY INTERNATIONAL, UNITED STATES OF AMERICA, *Where is the Justice for Me?: The Case of Troy Davis, Facing Execution in Georgia* (2007).
describe his trial as the “anatomy of a frame-up,” those less sympathetic toward his situation dismissed him as a “media’s latest baby seal.” Nonetheless, the prospect of these new technologies as a “road to democracy” gave hope to many: in the final hours of his life, Davis’s supporters tweeted, blogged, emailed, and posted pleas on his behalf. In the end, however, social media could not save his life. In order to understand why these methods did not prevail, we must consider both the contemporary story of Troy Davis and the historical story that ultimately decided its outcome.

On August 19, 1989, at approximately 1:00 a.m., Officer Mark Allen MacPhail was shot and killed in a Burger King parking lot at the intersection of Oglethorpe Avenue and Fahm’s street as he attempted to aid Larry Young, a homeless man who had been assaulted moments before the off-duty officer arrived. Troy Anthony Davis, who admitted to being present at the crime, fled the scene, and after being accused of the crime by Sylvester “Red” Coles, who was also present in the parking lot, surrendered to police and was arrested four days later on August 23rd. Davis was indicted on November 15, 1989, by the Superior Court of Chatham County, for the murder of Officer MacPhail. On August 28, 1991, Davis was convicted by a jury, and later the same day sentenced to death by electrocution.

On February 26, 1993, the Georgia Supreme Court affirmed Davis’s conviction and sentence. On March 15, 1994, Davis filed a Habeas Corpus petition; it was denied on September 9, 1997 by the state court. The petition was denied a second time by the Georgia Supreme Court on November 13, 2000. The Habeas petition was submitted to the U.S. District Court for the Southern District of Georgia’s Savannah Division, and denied on May 13, 2004. On September 7, 2005, the Eleventh Circuit Court heard oral arguments in support of the petition, and affirmed the District Court’s denial of federal habeas corpus relief on September 26, 2006.

On April 11, 2007, Davis submitted his certiorari petition to the United States Supreme Court, which was denied on June 25, 2007. On June 27th, the

Chatham County Superior court issued an execution warrant, and on July 5th, the Georgia State Department of Corrections scheduled Davis’s execution for July 17, 2007, at 7:00 p.m. On July 16, 2007, the Georgia State Board of Pardons and Paroles granted a 90-day stay of execution for Davis, and the following August, the Georgia Supreme Court granted Davis a discretionary appeal for a new trial. On March 17, 2008, the appeal was denied.

On September 12, 2008, the state parole board denied Davis clemency, but on September 23rd, the U.S. Supreme Court granted him a stay of execution. On October 14th, 2008, the U.S. Supreme Court refused to hear Davis’s appeal, however on October 24, 2008 the federal appeals court granted him a stay of execution. On April 16, 2009, the federal appeals court rejected Davis’s request for a new trial, on the following day the U.S. Supreme court ordered a federal judge to hear new evidence in the case. A hearing was convened in U.S. district court on June 23, 2010, to hear new evidence, but on August 24, 2011, the presiding judge rejected Davis’s request for a new trial based on that new evidence. On March 28th of the following year, the U.S. Supreme Court declined to hear Davis’s appeal of the district court’s ruling, and on September 6th, the Georgia State Department of Corrections set his execution date for September 21, 2011. On September 20th, 2011, the Georgia Board of Pardons and Parole denied Davis clemency, and on September 21st, after his appeals to the Georgia and U.S. Supreme Courts were rejected, Troy Anthony Davis was executed by lethal injection.14

At its inception, Davis’s trial attracted an expected amount of media attention. The Savannah Morning News reported on the case from 1989 through 1991, documenting Davis’s naming as a suspect, surrender, arrest, trial, and eventual conviction.15 The case gained significant media attention in 2003, when the Atlanta Journal Constitution began a series of articles and editorials...


raising questions about the trial and reporting on witness recantations. In 2007, a film produced for Amnesty International entitled *A Life in the Balance: Examining the Troy Davis Case* further documented the legal and moral issues the case presented. In 2009, CNN aired a story that highlighted the witness recantations and raised the question of whether Davis was a “cop killer or innocent man.” During the appeals process, this and other media attention helped to garner support from around the globe, eliciting calls for justice and clemency from prominent individuals such as Sister Helen Prejean, Pope Benedict XVI, and Archbishop Desmond Tutu.

New media also played a critical role in bringing the case into the public consciousness. Traditionally media outlets featured the case prominently on their web pages, and anti-death penalty organizations such as Amnesty International dedicated significant resources to reporting on Davis’s trial and appeals. Numerous African American and civil rights organization websites also documented Davis’s life and trial, and the power of social media was seen as a vital part of the campaign against his execution. “With the onset of technology and social media, our advocacy has gone digital,” proclaimed Curtis Johnson of the NAACP. “Perhaps one of our social media campaigns garnered as much worldwide participation as the ‘Too Much Doubt’ campaign. Started in support of Troy Davis, a man set to be executed in the face of overwhelming doubt, we campaigned for Troy using virtually every social network at our disposal.”

Davis’s case and the issues that it raised held a strong presence in the public


19. Letter from Sister Helen Prejean, author, Dead Man Walking, to State Board of Pardon and Paroles (June 26 2007).


21. Letter from The Most Reverend Desmond M. Tutu to the State Board of Pardon and Paroles (June 26 2007).

sphere, and contributed significantly to both public and private deliberations concerning racial justice and the death penalty.

Despite these efforts, Davis was executed, and his case raises serious issues for those who envision the Internet as a democratic technology, intoxicated by the apparent influence of social media on events in other parts of the world and the notion that the “combination of improved publishing technology and social networks is a catalyst for social change where previous efforts have failed.” In the aftermath of Davis’ execution, for example, supporters of this view contend that his case has led to an increased awareness of the injustice of the death penalty that could “have a corrosive effect on support for the death penalty down the road.” A less sanguine and ultimately realistic assessment holds that “by the rules of instant communication, social media failed. People tweeted, posted, and forwarded, but Troy Davis was still executed.” Like democracy itself, the technologies to which it gives rise offer no guarantees of rendering a system of jurisprudence just.

Research in social informatics supports this view. Deborah Johnson, for example, notes that there are many forms of expression and interaction embedded in the Internet that are non-democratic, anti-democratic, and unconcerned with democracy. Lincoln Dahlberg similarly argues that the technology itself is only incidental to popular participation in democratic processes: “The public sphere will not be extended merely through the diffusion of a new technological artifact. People must be drawn into rational-critical discourse before new technologies can be successfully employed to extend the public sphere.” The insights of Johnson and Dahlberg point to conflicts between political participation and technology that might very well be rooted in the modernist visions of Western democracy that shape our contemporary legal and political systems. These contradictions were cogently explicated in George Parkin Grant’s exploration of the tensions between liberalism and technology in his book English Speaking Justice:

In England, modern liberalism was above all the creed of the new bourgeois, in that the insistence on political liberties was related to the liberation of dynamic commercial technology, and thus with the expansion of that dynamism around the world. The claim to legal and

26. See Lincoln Dahlberg, The Internet and Democratic Discourse: Exploring the Prospects of Online Deliberative Forums for Extending the Public Sphere, 4 INFORMATION, COMMUNICATION & SOCIETY 615, 630 (2001).
The “difficulties” that confronted the English and French were even more pronounced in the Americas, where the destruction of indigenous cultures coupled with the “peculiar institution” of chattel slavery revealed the limitations of an idealized social contract that effectively excluded and exploited non-Europeans, and non-Christians.

These limitations continue to be revealed in contemporary intersections between difference, identity, and technology, as well as in the ways in which the legal and political institutions and forces that define and decide the meaning of “justice” continue to be caught between the abstractions of an incoherent social contract and the realities of an inequitable “Racial Contract.” Thus, faith in technology, like the faith in the reason it presupposes, is misguided precisely because it assumes an idealized vision of democracy in which race does not matter. The trial and execution of Troy Anthony Davis suggests otherwise, and we now turn to several critical perspectives on law, race, and media to offer an enlarged framework for enacting theoretical and practical strategies that facilitate political, economic, and social justice.

III. RE-SIGNING THE SOCIAL CONTRACT: MEDIA, RACE, AND THE LAW

Questions concerning the nature and character of justice are as old as Western civilization itself. In Plato’s *The Republic*, the dialogue between Socrates and Thrasymachus revolves around such questions, with Thrasymachus making the infamous claim that “justice is nothing else than the interest of the stronger,” and Socrates offering an idealized conception of justice as each one acting in accordance with his true inner nature for the benefit of all. The same debate is rehearsed again centuries later in the moral philosophies that gave rise to the notion of a “social contract,” in which the unfettered self-interest of individuals in a state of nature are juxtaposed against the need for constraints imposed upon them by institutional authorities. While the definitions of “nature” and the character of institutional authority are seemingly reversed in the two debates, they hold in common the claim that justice is ideally an art of social management that protects the interest of all and functions in service of the common good.

29. See John Wild, *Plato’s Modern Enemies and the Theory of Natural Law* (University of Chicago Press 1953), for discontinuities between classical and modern conceptions of rational justice. “In fact, as we shall attempt to show, Plato was a moral realist. As such, he must be
Historically, this art has been embodied in an adversarial culture and consciousness that has dominated legal theory and practice in the West. Grounded in rationality and practical reasoning, law has evolved largely as a set of attitudinal and institutional practices and procedures that aim at retributive instead of restorative ends. The violation of individual rights and liberties is addressed largely through processes of institutionally sanctioned discipline and punishment, and it is through this process that contractarian agreements are executed and sustained. While, ideally, such processes effectively protect the rights of all individuals, in reality they have excluded those “alien races” that the framers of English speaking justice have deemed less than rational, and less than human. Nowhere is this clearer than in moral incoherence characterized by the West’s domination and exploitation of people of African descent.

That moral incoherence exposes the failures of contractarian notions of justice by revealing how an idealized social contract has been enacted in what Charles Mills describes as a “Racial Contract.” “The ideal ‘social contract’ has been a central concept of Western political theory for understanding and evaluating the social world,” explains Mills. “I am suggesting, then, that as a central concept the notion of a Racial Contract might be more revealing of the real character of the world we are living in, and the corresponding historical deficiencies of it normative theories and practices than the raceless notions currently dominant in political theory.”\textsuperscript{30} This embrace of racelessness is one of two aspects of Enlightenment. The first is justice that illustrates its failure to acknowledge historical and cultural realties. The second is revealed in its privileging of retribution as the dominant strategy for framing issues of crime, criminality, and punishment.

\textit{In the Interests of the Stronger: Historicizing Capital Punishment}

Judith Kay argues that this privileging on retributive justice reflects a master narrative, one that denies its status as a historically constrained “story” and instead positions itself as an inevitable outcome of “natural” law. It is a story that, ideally, treats all who deserve punishment equally, and forms of punishment equitably. Historically, however, that has not been the case. As Judith Kay explains:

When Enlightenment philosophers tried to de-story their concepts of punishment, they wrote as if their views were free from the constraints of culture. This pretense resulted in a lack of critical insight into the

\textsuperscript{30} See Mills, \textit{supra} note 2, at 7.
question of who decides what counts as a harm (the ruling elites) and what harms would be designated as criminal actions (actions that harm those interests). The result is an ideological naïveté about the harsh injustices of the criminal justice system. Most Americans repeat the delusion that the criminal law targets for prosecution all intentional lethal actions and that the death penalty is reserved for the worst of the worst. These delusions are deadly.31

Kay’s analysis is decidedly rhetorical, and is specifically concerned with the moral and social implications of the death penalty as they are realized in the particular and concrete, in contrast to the ideal and abstract. She suggests that our contemporary investment in capital punishment is grounded in a set of beliefs about justice, crime, and punishment that remain rooted in antiquated Enlightenment beliefs, assumptions, and language about criminal justice. “By treating ethical concepts as if they made sense apart from any story, Enlightenment philosophers’ cover story became that they had no story. Today, punishment is discussed almost exclusively in Enlightenment categories.”32 Like the social contract to which it gave rise, the Enlightenment “story” of crime and punishment was, and continues to be, framed by an unspoken set of assumptions that define what we accept as reasonable, acceptable, and just, not only for ourselves, but for our fellow members of society as well.

Mills and Kay are by no means alone in their assessment of the moral incoherence of political theory and the legal and social institutions and practices to which it gives rise. Contemporary legal and moral philosophers have interrogated this rupture between idealized and enacted Critical theories in law, race, and media echo this analysis of the ideological and institutional impulses that enact and sustain privilege and perpetuate inequality through legal and political practices. Each of these perspectives offer powerful analytical lenses through which the trial and execution of Troy Anthony Davis might be viewed, and may provide a frame for understanding what many of his supporters experienced as a failure of justice and a reification of the interests of the stronger.

IV. REFRAMING TROY DAVIS: CRITICAL LENSES OF LAW, RACE, AND MEDIA

One of the most sustained and radical critiques of modernist legal and political theories have been advanced by Critical Legal Studies (CLS) scholars. Motivated by a postmodern critique of rationality and influenced by the progressive politics of the 1960s, critical legal theorists challenged both the rational foundations of law and the social practices it embodied. Theorists also offered a political and analytical critique of law that challenged its reliance upon

32. Id. at 10.
objectivism, foundationalism, and ruptures between legal and political conceptions of rights. CLS has an avowedly oppositional agenda that rejects liberal-democratic values and institutions, and argues for their radical replacement. Beginning with a leftist critique of law as a politicized hegemonic practice, they argue for its deconstruction, and evaluate it as a fundamentally repressive and regressive institution.33

Despite its powerful critique of contractarian law, the ideological agenda of CLS has not been translated into concrete legal and political advances for members of minority groups. Indeed, the inadequacies of CLS, when issues of race are concerned, led to the emergence of Critical Race Studies (CRS), an interdisciplinary critique of law and legal institutions that focuses on the lived experiences of people of color, those “alien races” historically exempted from signatory inclusion in the social contract. A key point of conflict between CLS and CRS is the radical rejection and replacement of enlightenment ideals by the former, and the belief that aligning those ideals with social practice offers a more constructive approach to transforming the Racial Contract into a legitimate and inclusive social contract held by the latter.34

The oppositional stance/perspective of CLS, which argues for informal and decentralized social and legal arrangements, runs the risk for CRS scholars of potentially replacing one idealized set of relations for another that has equally problematic assumptions of “race neutrality.” Scholars in Minority Legal Studies (MLS), a subset of CRS, articulates this concern in the following terms: “The two ideals, perhaps at an abstract level, share a vision of society in which citizens live their lives unfettered by oppression. However, the Minority Scholar ideal, by proposing institutional protections which CLS does not, moves from an abstract ideal to a realistic one.”35 Having never themselves experienced oppression, CRS scholars contend, “Crits” cannot conceive of the realities of racism and discrimination in anything other than abstract terms.

This resistance to abstraction and an emphasis on race and embodied knowledge has helped to cultivate an awareness of the need for self-reflexivity in CRS and those areas of inquiry that it has significantly influenced such as MLS, Feminist Legal Studies, and Critical Criminology. In her early analysis of essentialism in Feminist Legal Theory, for example, Angela Harris contends that


“legal theory, including feminist legal theory, has been entranced for too long and to too great an extent by the voice of ‘We the People.’ In order to energize legal theory, we need to subvert it with narratives and stories, accounts of the particular, the different, and the hitherto silenced.”

This focus on language and lived experience reflects the same impulse toward the rhetorical embodied in Kay’s critique of capital punishment, and is evident also in the critical work of scholars in the areas of crime and criminology.

Raymond Michalowski calls for a reconstructive agenda expressed in what he defines as “Critical Criminology” that emphasizes the “voices of immediate suffering.” Michael Coyle explicitly connects the concerns of Critical Criminology with the need for recognition of the powerful relationship between language and the social construction of racial identity. “The implication inherent in critical criminology is that if a racist ‘criminal justice system’ is present, then the racism lives in the language and importantly, given our age of political correctness, in a language that frequently does not sound racist.” The alignment of the symbolic with the structural that characterizes Critical Race studies is paralleled by an emerging body of inquiry and expression that addresses the role of media in the representation of criminality.

Craig Haney describes the emergence of fictionalized and media depictions of crime as “media criminology,” and argues that it “reinforces a dominant cultural narrative about the origins of violent criminality—one that implies something about the nature of the persons who perpetrate such crimes and the societal policies that are needed to properly address them.” Haney argues that this “master narrative” is not the result of media alone, and echoes the arguments of other scholars that place its roots and origins in 19th century notions of crime and punishment. While this narrative broadly influences attitudes toward violent crime, it is particularly troubling when race is involved, as it cultivates an “empathic divide,” particularly “when defendants of color are judged by white jurors, a dynamic that is likely to occur more often in death penalty cases because of the way in which death qualification disproportionately eliminates non-whites from participating on capital juries.” Media criminology thus reifies historical and institutional practices that perpetuate and sustain systems of domination and inequality through largely representational means.

This analysis is widely supported by critical media scholarship and creative work. “The targeting of ‘others’ has been a continuing element in public

40. Id. at 736.
punishment in the United States as well. Such official retribution has often targeted blacks and other minorities, whether in public lynchings, or death penalty cases, particularly if the victim is white,” explains Rachel Lyon. Further,

Dramatizing the villains, who must then be prosecuted and punished, has been a big business for print, television, broadcast news and even in the newer mediums of Internet entertainment. These media function as mediators of meanings, powerfully shaping the ways in which people understand our world by organizing information in such a way that the viewer/media participant forms perceptions over time about good and bad.41

Lyon’s documentary work reframes this understanding through an interventionist critique of the relationships between mediated construction of identity, social power, and racial privilege.42 Like critical studies of the law and race, critical studies of media offer a comparable account of identity, power, and privilege as they are shaped by mediated representations of difference. Influenced by the progressive agenda of cultural studies, critical media scholars argue that media are not comprised of objective rational agents who describe the world based on facts, evidence, and information. They are instead, made up of ideologically motivated individuals for whom the protection of privilege, whether consciously or unconsciously, influences understanding, perception, and decision making.43

This is made powerfully clear at the point where media and the law regularly intersect: the reporting of crime. Criminologist and critical media scholar Gregg Barak has explored this intersection extensively, and echoes the concerns of critical legal, race, and media scholars in his attempt to articulate a counter-hegemonic practice, what he terms a “replacement discourse,” which “is not simply critical and oppositional, but provides both a critique and an alternative vision.”44 Barak is suspicious of essentialized conceptions of race, crime, and justice, and articulates an approach to criminology that shows “the intertwined connections between individuals, activities that harm, and the whole of which we are a part.”45

Barak’s project intersects and amplifies the emancipative impulses of critical race and criminology theory, and affirms the emphasis in both of these areas of inquiry for an alignment of the structural with the symbolic. It calls for a

42. See Race to Execution (Rachel Lyon 2007); Internet Documentary: Juror Number 6 (Rachel Lyon 2009).
45. Id.
reflexive account of the intersection between law and media that recognizes how “the retelling of stories of crimino-legal justice reveal [sic] the interplay between media consumption and the social construction of crime and danger.”

His “interventionist” critical agenda, calls for a reframing of criminality that challenges the narratives that we have inherited and, often unconsciously, consumed as true, just, and real. Barak’s observations provide a powerful lens through which to view the trial and execution of Troy Anthony Davis, precisely because they point to both the possibilities and problems of the assumptions underlying the narrative turn in critical research.

One of those assumptions is that an enlarged public sphere of discourse and knowledge, the inclusion of more voices, can help to bring about a more equitable and just society. While the inclusion of multiple voices might be a necessary precondition for a more democratic society, it is hardly sufficient: indeed, this has precisely been the case with the rapid technological advances that have transformed traditional media.

Hence, the mass production of knowledge, or what passes for it, which was once primarily confined to the writings and research findings of the professionally trained experts or disciplinarians, today, by contrast, include widely disseminated information propagated by nonexpert, and often, unadulterated ideological sources, such as those found in fiction, film, and television, not to mention the ever expanding and omnipotent Internet and World Wide Web.

Barak’s project is both instructive and prescient. It is instructive in that it opens up the possibility of understanding the politics of racial justice in terms of its institutional, ideological, and individualized forms. It is prescient in that it presages one of the most perplexing and contested dimensions of the Troy Davis case: the failure of traditional and emerging media technologies to intervene successfully in his eventual execution.

After being convicted and sentenced to death by a jury of his peers, the legal considerations afforded Troy Anthony Davis in the appeals process did not ultimately address the question of whether he was guilty or not guilty: only if he should be put to death or kept in prison for the rest of his life. That the state’s decision to enact the ultimate punishment was highly contested and by no means inevitable is evidenced by the fact that there were numerous stays during the twenty years that Davis spent on death row, and that several appeals for reconsideration of evidence were granted. It is also suggested by the lack of unanimous decisions in the case. Yet despite this uncertainty and doubt, as well as the significant outpouring of support for clemency, Davis was ultimately put to death.


47. Id. at 481.
The reasons for the decision to execute Davis were both procedural and statutory. Among other things, presiding judges cited Davis’s failure to present evidence at the original trial, jurisdictional issues, and lack of witness credibility as reasons for rejecting his appeals and requests for reconsideration. Davis’s case was also hampered by the lack of support for post-conviction defenders enacted in 1995, and the legislative constraints of the Anti-terrorism and Effective Death Penalty Act passed in 1996. But the reasons given that led to Davis’ execution, although sufficient to justify the decision, did not necessarily require the result. Indeed, at any point in time, an alternative set of reasons could have been adopted that would have justified different decisions: a lack of physical evidence (no murder weapon was ever found), inconsistent witness testimony, evidence of police coercion, witness recantations, and evidence that his accuser may have himself committed the crime.

The question of why this set of reasons did not result in reasonable doubt about the necessity of executing Troy Anthony Davis might be partially answered by Kay’s analysis: that they do not fit our cultural “story” about the death penalty. “A great deal of confusion in thinking about the death penalty stems from the denial of the story dependence of any rationale for punishment. Indeed, the repudiation of story has had grave consequences for the practice of punishment.” Beyond the legal and procedural concerns raised by this alternative set of reasons, explains Kay, there are concerns that challenge the “cover story” of who we are as a society, and dismisses the mistreatment of the disadvantaged as inconsequential. “In the United States, the cover story says that there is no structural injustice in the land of liberty and equality. It denies that people suffer disadvantages because of their class, sex, or race, and that such mistreatment—if left unchallenged—can ruin lives.” In Troy Davis’s case, a life was not simply ruined: it was ended.

Critical theories of law, race, and media all offer powerful insights into the institutional and ideological impulses that framed and constrained the Troy

48. For the legal arguments presented on Davis’s behalf and rulings associated with his appeals see Davis v. State, 426 S.E.2d 844 (Ga. 1993); Davis v. Turpin, Civ. Action No. 94-V-162; Davis v. Turpin, 539 S.E.2d 129 (Ga. 2000); Davis v. Terry, 465 F.3d 1249 (11th Cir. 2006); Docket for 06-1407 Supreme Court of the United States.


50. See Elizabeth Schulte, Justice Denied Again for Troy Davis, SOCIALISTWORKER.ORG, March 28, 2008, http://socialistworker.org/2008/03/28/justice-denied-troy-davis (Georgia State Supreme Court Justice Leah Ward Sears, in her dissenting opinion, questioned the court’s refusal to grant him a new trial: “If recantation testimony, either alone or supported by other evidence, shows convincingly that prior trial testimony was false, it simply defies all logic and morality to hold that it must be disregarded categorically”).

51. See Kay supra note 28, at 1-2.

Davis case, yet fail to achieve the *praxis* they theorized. All of these perspectives, however, even as they contest the objectivist and essentializing impulses of modernism, nonetheless embrace one of its most compelling epistemological commitments: an investment in what Jürgen Habermas defines as the “emancipatory cognitive interest.” Habermas affirms the modernist commitment to rational discourse as a precursor to the creation of a democratic polity, arguing that it cultivates the capacity for self-reflexivity that is at the heart of public and critical discourse.

The point at which Habermas and the critical theorists of race and criminology mention above depart from Enlightenment rationalism is the faith in the power of discourse to transform institutional structures. Underlying Habermas’ emancipative interest is a belief in the efficacy of communication for the mediation of individual, ideological, and institutional conflicts. Thus, Habermas envisions an “ideal speech situation” as the culmination of the modernist enterprise, a situation in which, given equal access to the public sphere, practical reasoning and persuasion can be vehicles through which contractarian guarantees of justice and equality can be achieved.

The Habermas ideal is, however, just that: an ideal. And the realities of the Racial Contract, as well as the critical interventions of legal, race, and media critics, not only stand in juxtaposition to the rationalist orientations of modernism, but also render problematic one of the celebratory commitments that it shares with these critical projects: that, if given the “right” information, individuals and institutions can be transformed through reasoned discourse. This is an unspoken assumption of much contemporary criticism, and it presupposes that racism is ultimately a problem of rational deliberation. As such, it is a problem that can be addressed adequately through education: that if “reasonable” people are given the “correct” information, they will make the “right decisions.” The Troy Davis case suggests otherwise.

The Davis case challenges this celebratory belief in the power of persuasion and intellectual understanding, central to Enlightenment thinking and still nascent in the “rhetorical turn” that characterizes the critical projects of law, race, and media. It illustrates the fact that, despite a preponderance of evidence that pointed to reasonable doubt; despite a plethora of examples of the inequitable application of the law in death penalty cases when race is involved; despite an enormous public outcry expressed through both traditional and new

media demanding that his life be spared; despite all of this, Troy Anthony Davis was put to death. For some, his death represented the righteousness of retributive justice. To others, it caused a sense of resignation and disbelief leading to a loss of faith in reason, fairness, and the basic principles and practices of American law. For the authors of this essay, his death represents an important opportunity to interrogate and rethink the problems of how law, race, and media might enhance our understanding of the possibilities of restorative justice.

V. EXECUTING DEMOCRACY: FROM RETRIBUTION TO RESTORATION

It is not unreasonable to argue that the decisions that led to the execution of Troy Davis were motivated by race. Indeed, there is ample evidence to indicate that race continues to play a significant role in capital cases. Baldus et al. in their analysis of the relationship between race and capital punishment in Pennsylvania conclude “the problem of arbitrariness and discrimination in the administration of the death penalty is a matter of continuing concern and is not confined to southern jurisdictions.”\(^56\) Peffley and Hurwitz, in their analysis of the effect of arguments that emphasize the unfairness of the death penalty draw even more troubling conclusions. “When confronted with the argument that the death penalty is racially unfair, whites who believe that black crime is due more to blacks’ dispositions than to a biased justice system end up rejecting the racial argument with such force that they become even more supportive of the death penalty.”\(^57\) At both the institutional and attitudinal level, race continues to influence how justice is understood and enacted in American society.

Peffley and Hurwitz suggest that, in contrast to white resistance to persuasion, blacks are more likely to be influenced by the fairness issue in light of their historical experience with the justice system. Yet, in the Davis case, this conclusion is undermined by the fact that both the jury that tried, convicted, and sentenced him to execution, and the Board of Pardons that affirmed their decision, were racially mixed. The Davis case was, on the surface, a stereotypically racialized case of a black man accused of killing a white police officer in the South, yet it was also at a deeper level, a case that simultaneously challenges static notions of racial identity and difference, and questions the effectiveness of rational discourse in cultivating a just and equitable society. It points to the power of deeply held beliefs about race and justice to influence and


motivate action, and suggests that a more nuanced understanding of race might be needed to facilitate the movement of critical inquiry toward social transformation.

It is worth noting that despite the racially mixed composition of both the original jury and the Board of Pardons, whites outnumbered blacks. To the extent that the two races maintain different perspectives on crime, punishment and justice itself, such inequality tends to reproduce existing power relations even as appearing to offer the possibility of fairness.

To the extent that the perspectives are reproduced in the processes of the jury and parole board, they represent the continued institutional power of whiteness the imposition of this observation is underscored by two areas of inquiry that hold promise for that movement: the study of implicit bias and research on the rhetoric of racism. Based upon an empirically grounded “Implicit Association Test,” implicit bias research reveals the persistence of underlying beliefs about race and difference, and how they unconsciously influence individual and institutional decision-making. “The types of racial bias revealed in this testing have been found to affect all aspects of the criminal justice system,” explains David Harris, pointing to research that examines probation officers’ perceptions of offenders of different races, jury attitudes, and even judges’ sentencing decisions. He concludes, a fortiori: “If experienced judges cannot seem to avoid racial bias, it is hard to imagine that death penalty jurors are exempt from such influences.”

Most importantly, implicit bias research illustrates how these beliefs cut across established categories of physical difference and, by virtue of their unconscious character, actively resist persuasive, argumentative, and even critical interventions. It affirms a critical conception of racial identity that is closely aligned with the important distinction drawn by Mills between white as a physical category, and whiteness as a way of knowing and being: “Whiteness is not really a color at all, but a set of power relations.” The heuristic power of Mills’s observation is important, for it recognizes that while people of European descent have historically been the beneficiaries of the Racial Contract, they have not been its only signatories: “All people can fall into Whiteness under the appropriate circumstances,” he writes, citing as an example the intra-racial genocide that occurred in Rwanda in 1994. For Mills, the Racial Contract is not a rejection of Enlightenment ideals, but a racially informed critique of its unspoken assumptions and ideologies.


59. See Mills, supra note 2, at 127.

60. See Mills, supra note 2, at 128-29.
(Re)Signing the Racial Contract

Research on the rhetoric of racism also explores the constitutive power of whiteness and questions the efficacy of rational discourse in the achievement of racial reconciliation. At its most sanguine, the research affirms the reconstructive impulses of critical race theory in its recognition that a purely oppositional critique remains complicit with oppression, and in its affirmation of coherence between principle and practice as an alternative to that complicity. At its most skeptical, it points “to the limitations of rational rhetoric to address the realities of race, as well as the inability of law and politics to extend to people of African descent the inalienable rights ostensibly enshrined in the foundational beliefs and expressed in their forensic and deliberative declarations.” It questions the efficacy of rational rhetoric and practical reasoning in the critique of racial identity and division, positing that the history of rhetorical inquiry as it relates to race clearly illustrates the inadequacy of finding and using “the available means of proof, “ and suggests instead that racism is more likely a problem of “psychiatry” than “persuasion.”

Like Critical Legal Studies, research on the rhetoric of racism offers a racial critique of contractarian justice, but follows the approach of Critical Race Studies in its suspicion of critical deconstruction that lacks a reconstructive agenda. Like CRS and Critical Media studies, it considers the roles of language and symbolic representation in the social construction of race, and cautions against the essentializing impulses of oppositional notions of difference and identity. Such notions obscure the degree to which the dominant and the dominated can be complicit in systems of oppression, whether through language, thought or action. In its most recent articulation it aligns the moral and philosophical social critique of Mills’s Racial Contract with the empirical findings of symbolic racism and implicit bias research.

The critical project of the rhetoric of racism affirms the notion that limiting our discussion of race to identity and physicality limits the available means of political transformation, resulting not in an idealized democracy envisioned in Enlightenment discourse, but in what Joel Olson calls “white democracy”: “The problem with limiting our understanding of race to personal identity is not that it leads to a politics of resentment, victimization, or balkanization, as many critics of identity politics argue, but that it leads to very little politics at all.” The critical project of the rhetoric of racism calls our attention to the extent to which

61. See Mark Lawrence MacPhail, Zen in the Art of Rhetoric: An Inquiry into Coherence (State University of New York Press, 1994).
64. See Joel Olson, The Abolition of White Democracy 6 (University of Minnesota Press, 2004).
oppositional criticism too often reifies the rationalizations of Enlightenment reason by privileging abstract and idealized possibilities instead of practical and empirically verifiable realities.

The rhetoric of racism reveals that, in the case of race, rhetoric, like reason, has failed in Western theory and practice to translate democratic thought and discourse into an embodied social practice. It nonetheless also acknowledges that in the absence of an embodied politics, intellectual inquiry can still offer a productive vehicle for articulating strategies of transformation that connect the personal with the political. This connection is important to our understanding of law, race, and media, precisely because it considers the limits of institutional and representational changes that are divorced from and embody politics. The transformation of law, race, or media may begin with institutional practices and bodies, but if those transformations fail to find expression in the lived experiences of the individuals who interact within their contexts change will not occur.

Critical theories of law, race, and media provide a starting point for such transformations, and we here return to George Parkin Grant’s consideration of English-speaking justice to suggest some productive future directions: “At a time when massive technological advance has presented the race with unusual difficulties concerning political liberty, what was needed from our academics was an attempt to think through all that was valuable from the great western traditions which could help us in dealing with these difficulties.” It would appear that we are today confronted with the same conditions that gave rise to the legal and political theories and practices that marked the period of history that produced the difficult and dangerous “story” that contains and constrains our understanding and experience of racial (in)justice, crime, and punishment. The question before us is whether we can learn from that history, or if we will be condemned to repeat it.

Grant’s analysis suggests that a return to contractarian values and notions of justice may be our best hope for the future of the race, and for the reconciliation of the Racial Contract, and Mills also infers that this might well be the case. Mills argues that the Racial Contract is not simply a rejection of deconstruction of Enlightenment ideals, but an attempt at their reconstruction, a call for coherence between principles and practices. The Racial Contract “criticizes the social contract from a normative base that does not see the ideals of contractarianism themselves as necessarily problematic but shows how they have been betrayed by white contractarians,” explains Mills. “Thus it lays claim to truth, objectivity, realism, the description of the world as it actually is, the prescription for a transformation of that world to achieve racial justice—and invites criticism on those grounds.”

65. See Grant, supra note 26, at 92.
66. See Mills, supra note 2, at 129.
Mills’s Racial Contract is thus a restorative vision of justice, in that it focuses “on the harms caused by the offense,” and seeks “to repair the damage and restore broken relationships.” It is a “replacement” story of justice, one that emphasizes ethics, morality, and relationships over procedure, one that, evidently, we as a culture have difficulty accepting because it challenges our belief that our institutions truly serve the common good, and not simply the interests of the stronger. It is a story that might have led to a very different ending to the final chapter of Troy Anthony Davis’s life. It is a story that invites us to consider carefully the possibilities and problems of law, race, criticism, and the promise that technology holds for the cultivation of deliberative democracy.

The unfulfilled promise of social media romanticized in the Troy Anthony Davis case reminds us that our commitments to legal, racial, and representational change remain incomplete unless realized in embodied practices. They invite a rethinking of race that takes us beyond the biological determinism and essentialist impulses of understanding racism in terms of white people, and instead recognizing it as a manifestation of whiteness. This rethinking is, we believe, necessary for a reconciliation of the oppositional tendencies of thought and practice which perpetuate racial and retributive (in)justice, and contribute to what Olson describes as “White Democracy”: “The radical democratic ideal, then, is neither the refusal of recognition of race nor the equal recognition of cultures or races but the refusal of recognition of whiteness. Such a refusal opens space to create new forms of identity—for those who are white and those who are not—amidst a reinvigorated public sphere.” Olson’s claim sounds eerily like those of new media enthusiasts who believe that the Internet and other forms of social media can open new spaces for democratic participation in the public sphere. Yet in the absence of an embodied politics that challenges racial and digital divisions, the degree to which either claim can be translated from an abstract ideal into a concrete practice, remains to be seen.

In Executing Democracy: Capital Punishment & the Making of America, 1683-1807, Stephen John Harnett’s explication of “the rhetorical history of a very hard choice” magnifies the connections that we have drawn here between law, race, and media when he noted that

[T]he history of the death penalty converges on this period of American history with the dawn of the culture industry. As new forms of mass-produced persuasion and entertainment began to flourish, and as elites continued to address the masses from the gallows, so the voice of these documents began to change.

---

67. See Kay, supra note 28, at 9.
68. See Olson, supra note 58, at 123.
Excluded from these voices, except perhaps as objects of their stories, African Americans cultivated an embodied politics that enlarged the limited notion of equality envisioned by the British colonists, persistently calling for the colonizers to be true to what they “put on paper.”

This call for coherence was echoed in the abolitionist discourse of Frederick Douglass and in the civil rights rhetoric of Dr. Martin Luther King, Jr., and informs the emancipative projects of critical theories of law, race, and media. Their call for a system of legal justice that connects the personal with the political, gives voice to the silenced, and seeks a reconciliation of the contradictions of a “post-Revolutionary nation struggling to live up to its professed principles.”\textsuperscript{70} This might be our best--if not only--chance to heal the divisions, social and digital, that continue to separate us from the better aspects of our natures.

One of the most powerful examples of the translation of this theoretical project into embodied action can be seen in the words of Charles Ogletree, presented in a letter to the Georgia State Board of Pardons in July 2007, requesting the commutation of Troy Anthony Davis’ death sentence. The letter presented legal and empirical arguments as justifications for the request, but it also drew upon Ogletree’s own personal experience of violent crime: the murder of his sister Barbara Jean Ogletree Scoggins.

\begin{quote}
    It took a great deal of reflection and prayer to accept that my younger sister had been murdered. This brutal fact haunts and pains me to this day. My commitment to finding the person responsible for her death has not diminished. I have offered a reward for information leading to an arrest. While Barbara’s killer should be punished, taking that person’s life based on the kind of self-contradictory and recanted statements of unreliable witnesses found in the Davis case would not be a solution that Barbara, my family, or I could endorse.\textsuperscript{71}
\end{quote}

Six days later, the Georgia Board of Pardons granted Davis a 90-day stay of execution. While there is no way of knowing what effect Ogletree’s words might have had on the Board’s decision, his letter clearly reflected a commitment to reconcile tension between personal and political interests in the pursuit of restorative justice.

Five years later, in a letter released on the Internet reportedly written by Davis, he made a similar call for restorative justice:

\begin{quote}
    I can’t even explain the insurgence of emotion I feel when I try to express the strength I draw from you all, it compounds my faith and it shows me yet again that this is not a case about the death penalty, this is
\end{quote}

\textsuperscript{70} See Letter from Charles Ogletree, Chairman of the Board of the Southern Center for Human Rights, to Garland Hunt and the Georgia State Board of Pardons and Paroles (July 11, 2007).

\textsuperscript{71} Id. at 210.
not a case about Troy Davis, this is a case about Justice and the Human Spirit to see Justice prevail.”72

Unlike Ogletree’s words, this plea for justice fell on deaf ears, and on September 21, 2011, Troy Anthony Davis, finally free, was silenced forever.

In the final statement made before that silencing, Davis poignantly expressed the point that we ultimately wish to make in this essay: “All I can ask . . . is that you look deeper into this case so that you really can finally see the truth.”73 What critical studies of law, race, and media suggest, and our contemporary practices that shape crime, criminality, and justice confirm, is that the truth can be found in the Thrasy Machean assertion of justice: that is, indeed, little more than the interests of the stronger. But the life and death of Troy Anthony Davis reveals other truths: that human beings are capable of profound forgiveness and compassion, and that restorative justice is not simply an ideal, but also a possibility.

VI. CONCLUSION

Throughout this essay we have focused largely on the stories of race, crime, and justice as they have framed the life and death of Troy Davis, but we have been largely silent about the life and death of the other actor involved in these events: Mark MacPhail. While we cannot do justice here to the complexity of his story or history, we can acknowledge that he was a white police officer who gave his life in attempt to aid another man, himself the victim of a violent crime. He had a wife and children, and he chose a profession that he knew might inevitably put his life in danger. His final deeds were, by any account, heroic. We have no doubt that he believed in the possibility of a society in which the lives of all individuals were worth protecting, in which all individuals were worthy of justice. Charles Ogletree characterized MacPhail in his letter to the Georgia Board of Pardons: “As a respected police officer no doubt committed to peace, justice, and fairness, it is terribly difficult for me to believe that Officer MacPhail would have endorsed the decision to execute Mr. Davis despite a complete absence of physical evidence or reliable eye-witness testimony.”74

Although we cannot know what Officer MacPhail might have endorsed, we do know what his family believed: that Troy Davis was responsible, and that he deserved to be executed. “We have followed the law, played by the rules, and those that are in positions of power have made their decisions along this long


74. See Ogletree, supra note 65.
sorrowful trip,” observed MacPhail’s youngest sister, Kathy McQuary. She continued, stating that

It is time to deliver the appropriate punishment and show our communities we believe in them and we will do what we need to do to ensure we are all safe. The rules are in place for a reason, we all have to abide by them. They are there for the safety of ALL of us.75

Like the members of the Georgia State Board of pardons and all those who supported the execution, the MacPhails believed that Davis had violated an agreed upon social contract and, as a consequence, deserved to suffer the highest penalty.

Yet, as we have shown, that contract has not in its execution truly applied to all. Following the law, playing by the rules, and trusting the judgments of the powerful and the privileged is no guarantee of justice. Still, we conclude with a sense of hope, not in our institutions, ideologies, or strategies of inquiry, but in the decisions made by individuals seeking to find a justice that lives in both principle and practice, a justice based not on retribution, but on a restoration of our broken beliefs, communities, and lives. We turn to the case of Russell Brewer, the murderer of James Byrd, who was also executed by the same system of retributive justice that took the life of Troy Davis. Brewer’s execution shows again, that race, crime, and justice, cannot be adequately understood in black and white terms.

On September 21, 2011, the day that Troy Davis was executed, Byrd’s family pleaded that Russell, an unrepentant white supremacist, be spared76. That their request was denied sadly reflects the same voicelessness of the millions who sought to spare Davis, but the Byrd family’s words suggest that the Racial and Social Contracts might one day be reconciled, if not through intellectual inquiry or institutional transformation, then through individual acts of forgiveness and compassion. “If I saw him face to face, I’d tell him I forgive him for what he did,” said Byrd’s sister, Betty Boatner. “Otherwise I’d be like him. I have already forgiven him.”77 Byrd’s son’s words also offer hope for the possibility of a society no longer blinded by retribution and revenge, in which restorative justice is possible: “I hope that they will stand back and look at it before they go down that road of hate. Like Ghandi said, an eye for an eye and the whole world will go blind.”78

DATAMINING FOR GOLD: SOCIAL MEDIA AND SOCIAL CAPITAL IN A POSTNATIONAL GLOBAL MARKET

Susan H. Stephan*

Abstract

Tools of social media are becoming the most prevalent venues for online content sharing and creation worldwide. Both the manner in which the online social interaction of individuals and groups is targeted through marketing based on Internet behavioral tracking, and the use of the resulting data that is mined through tracking, ultimately can affect the way diverse groups of people perceive and interact with each other. Behavioral tracking online also has economic ramifications based on the end-use of mined data. As the enormous financial incentive to gain control of the globalized Internet society and its goldmine of data become obvious, the attempts at regulation and laws that control the environment become at the same time critical and overwhelming.

The consequences of online regulations on the long-term well-being of the world economy are potentially endless. I will examine the small portion of the socio-legal significance of online member communities in the global market that relates to social and economic capital created by online networking and associated datamining. I also will briefly discuss a few trends of the developing laws of the Internet society in today’s globalized environment.

I. INTRODUCTION

The number of visitors to cyberspace, both for business and social interactions, is increasing every year. An estimated 2,267,233,742 people, or more than 30% of the world’s population, were Internet users by the end of 2011.¹ This represents a 528% growth as compared to 2000.² Nielsen Online reports that two-thirds of the Internet population visit social networking or blogging sites.³ A reported 1.2 billion users currently participate in social

---

² Id.
networks. Spending time as part of an online “member community” engaged in blogging and social networking is now the world’s fourth most popular Internet activity. Member community activity has surpassed the use of e-mail and is only exceeded by online searches, portal visits, and computer software application use. In most months since 2007, the number of Internet users engaging in social networking exceeded the number of visitors to pornography sites, which formerly was the number one online activity, at least in the United States and the UK.

Within the member community realm, the social networking site Facebook is the fastest growing and most popular social network in the world. Although Facebook users are now emerging everywhere, two of the top four most drastic increases in users between 2008 and 2011 occurred in Indonesia and the Philippines. The development of social networking norms in those locations is likely representative, at least to some extent, of the growth in adoption of online member communities in post-colonial states across the world. Indonesia and the Philippines were victims socially and economically of the 1997 Asian financial crisis, a fact which has implications related to the Internet as well as globalization.

I will briefly address the Asian financial crisis and the post-crisis economic backdrop of Indonesia and the Philippines. Then I will discuss the Internet as a society that is comprised of increasingly global online member communities that are strengthened by social networks. Working primarily within the framework of Benedict Anderson’s concepts of the “imagined communities” of nation as analogous to the imagined member communities related to social networks, I will focus on social networking in post-1997 Indonesia and the Philippines. Finally, I

---

5. Nielsen, supra note 3, at 1.
6. Id.
8. ComScore, supra note 4, at 8.
9. Eric Eelden, Indonesia, Taiwan, Philippines and India Gained the Most Facebook Users In Asia Last Month, INSIDEFACEBOOK.COM (Nov. 12, 2009), http://www.insidefacebook.com/2009/11/12/indonesia-taiwan-philippines-and-india-gained-the-most-facebook-users-in-asia-last-month (stating that the top five countries through 2009 were Indonesia, Australia, Taiwan, the Philippines and India). See also Tonyo Cruz, Brazil, Indonesia, Philippines lead world in Facebook user growth, TECHWIREASIA.COM (May 30, 2011), http://www.techwireasia.com/1258/brazil-indonesia-philippines-lead-world-in-facebook-user-growth (stating that the top three countries through 2011 were Indonesia, the Philippines and Brazil).
will examine Internet society’s potential role in globalization through the social capital created by social networking as well as the economic significance of online member communities as they develop in today’s globalized environment.11

II. INDONESIA, THE PHILIPPINES, AND THE ASIAN ECONOMIC CRISIS

In Thailand, mid-1997, a run on Thai currency (the baht) resulted from slowing export business, increasing central bank credit to weaker institutions, and a dimming financial picture.12 The monetary crisis in Thailand quickly spread to similarly situated, East Asian economies including South Korea, Malaysia, Indonesia, and the Philippines.13 Indonesia was one of the hardest hit by the crisis.14 The Indonesian government passed the Indonesian Bank Restructuring Agency (IBRA) in 1998, which eventually took over thirteen weak banks, provided capital to other banks, supported several bank mergers, and closed forty-eight banks outright.15 Unfortunately, political turmoil accompanying the fall of then-president Suharto, in addition to questions about the effectiveness of Indonesia’s financial sector restructuring, resulted in continuing economic woes.16

The Philippines also fell victim to the crisis but was not as devastated economically as was Indonesia.17 The financial sector in the Philippines was affected by the crisis, with credit rates increasing and credit sources drying up.18 Eventually its currency (the peso) was devalued, resulting in inflation,19 and with the previously decreasing poverty rate holding steady, unemployment rates rose.20 Fortunately for the Philippines, it was not as deeply affected by the crisis as Indonesia.21 Now, both Indonesia and the Philippines are making strides

---

11. Although by no means unrelated, the controversial role of foreign direct investment, the World Bank, and IMF policy are outside the scope of this paper. Similarly, this paper does not touch on the potential connections among globalization, the 1997-1998 Asian financial crisis, and the 2008 global financial crisis that had significant impact in the United States as well as much of the rest of the world.
14. Id. at 28.
15. Id.
16. Id.
18. Id. at 3-5.
19. Id.
20. Id. at 6-8.
21. Id. at 2.
economically, although not without significant external investment in what remains a cautious environment.\textsuperscript{22}

In addition to the liberalization of international trade barriers in the several decades leading up to the Asian financial crisis, investment into developing countries, and foreign investment generally, had skyrocketed.\textsuperscript{23} Although analysts cannot agree as to the exact cause of the financial crisis, one important element seems to have been the significant external loan debt that had supported the impressive growth in the East Asian economies beginning in the late 1960s and early 1970s.\textsuperscript{24} When foreign-lender confidence in the ability of the Asian governments to continue to repay the debts began to falter, runs on the local currency resulted, and the concerns about loan default became a reality.\textsuperscript{25}

\textbf{A. The Role of the Internet}

In 1997, before social networks began to spread across the increasingly globalized online world, the Internet was undoubtedly a cultural factor that played a part in the growth of the economic drive of globalization. The Internet as a technology might also have had a role in the crisis, both as a facilitator of electronic financial transactions and as a source of instant and far-reaching reports of the economic free-fall conditions in East Asia. Post-crisis, the Internet continues to play some role in globalization and its contribution to a growing economic and social interdependence.

\textbf{B. Cyberspace as a Society}

Before analyzing the causes and effects of active online member communities in post-crisis Indonesia and the Philippines, it is worth considering the society in which I propose that these communities operate. To contextualize online communities within cyberspace as a society, I would adopt the definition of “society” that describes “a group of humans broadly distinguished from other groups by mutual interests, participation in characteristic relationships, shared institutions, and a common culture.”\textsuperscript{26} It is important to distinguish society in cyberspace as separate from the broader definition of society as “the totality of social relationships among humans”\textsuperscript{27} and from the narrower concept of Benedict Anderson’s “nation” or “nation-state.”\textsuperscript{28} Anderson’s imagined community of

\begin{footnotesize}

\begin{itemize}
  \item \textsuperscript{22} Kyung, \textit{supra} note 13, at 178-84.
  \item \textsuperscript{23} \textit{id.} at 25.
  \item \textsuperscript{24} \textit{id.} at 25, 165. Even by 2000, the International Monetary Fund (IMF) and the World Bank had loaned the equivalent of tens of billions of US dollars to Indonesia.
  \item \textsuperscript{25} \textit{id.} at 25.
  \item \textsuperscript{26} Society, \textsc{The Free Dictionary}, http://www.thefreedictionary.com/society (last visited Jan. 20, 2012).
  \item \textsuperscript{27} \textit{id.}
  \item \textsuperscript{28} Benedict Anderson, \textsc{Imagined Communities} 6 (2d ed. 1991) [hereinafter \textsc{Imagined Communities}].
\end{itemize}
\end{footnotesize}
nation may be a component of an individual’s place in the cyberspace society, but “society” and “nation” are not interchangeable. Anderson defines the nation as an “imagined political community – and imagined as both inherently limited and sovereign.” Although society and nation might share the similar features of shared relationships, institutions, and culture, a society would typically be much broader than a single nation. By my definition, society is comprised of a number of different communities, one of which might be the imagined community of nation. Thus, a “nation-state” combines the imagined political community of nation with political sovereignty within a particular geographical territory. Similar to the way in which a community is a subset of a given society, a nation-state would most often be a subset of the imagined community of nation. I propose that, within the preceding framework, the Internet makes up a society of humans, each of whom might be a citizen of a particular nation-state, have a concept of his or her nation, and still belong to a common culture online.

The Internet as we know it today, in the form of the World Wide Web, has existed for approximately twenty years. Given its relatively short life span, it does not seem unreasonable to compare the developing online community to a “primitive” society in terms of developing social order. Some academics view ordering to be native to a new society and, at first, an open social network that is regulated by the concepts of reciprocity and of fitting within the social and economic norms of the prevailing culture. This concept would seem quite appropriate in terms of an Internet-based social network as well as a more traditional view of a new society based on a grounded geographical location.

In the 1920s, Bronislaw Malinowski studied what he saw as a primitive community in Melanesia in an attempt to classify the norms and rules of that culture, to determine “the nature of the binding forces, and to classify the rules according to the manner in which they are made valid.” Malinowski concluded that the primary incentive for individuals to follow their rules was to remain within the social and economic order of the society. There are many indications that the global Internet community parallels Malinowski’s primitive society. For example, social norms related to communications through instant messaging, blogging, and social networking websites have developed, as have

29. Id. at 6-7.
30. Id. at 6.
31. However, the ARPA (Advanced Research Projects Agency Network) developed by ARPA of the United States Department of Defense, the world’s first operational packet switching network and the predecessor of the global Internet, dates back to 1969.
33. Id. at 41, 58.
34. See, e.g., Jeremy Keehin, Social Norms on the Web: How to Create Productive Digital Communities 1 (June 7, 2010), http://thekeesh.com/docs.norms.pdf.
The Internet also has its own culture to which users must conform by following “net etiquette” or “netiquette.” This series of norms and proffered rules of the web might indicate that the Internet community engages in rule-generation and inducement to comply. Similarly, commentators have suggested that social ordering or “private government” functionality takes place through institutional frameworks and through open social networks, the latter being most often regulated by concepts of reciprocity and “tacit understandings.”

In addition to cultural norms online, there is a developing – but far from developed – body of legal norms that comprises “cyberlaw.” Current regulations intended for the online environment are as much focused upon Internet service providers as they are private actors. Traditionally, law involves a centralized sovereign actor that exerts power within its territorial boundaries. The Internet, however, poses challenges to this traditional concept of governing law because of the broad reach of content over geographical borders. No single nation, nation-state, or community controls the broader Internet society. The lack of a centralized governing structure for most of what occurs online, in combination with a rapid change in the technologies that support online activity, make legal rules difficult to apply to the Internet.

One commentator, Michel Foucault, considered both social and legal norms, and he described the concept of “society” as “one of the great discoveries of...
political thought at the end of the eighteenth century,"²⁴² comprised of a complex reality with its own laws and reactionary mechanisms in addition to the territory, domain, and subjects that go along with society. The global online community seems to fit squarely within Foucault’s concept of society, based on the way in which the Internet functions as a territory in cyberspace that hosts a separate reality with its own set of norms. Foucault went on to discuss the importance of examining the relationship between space and power in a given society, particularly with the advent of new technologies that beget economic processes. When examining this relationship, Foucault’s methodology of a relevant “discourse” necessarily comes into play.

Foucault’s discourse is not the discourse of conversation and ideas; rather, it is the set of practices obeying certain rules within a structure.¹⁴⁵ Foucault’s version of discourse is more about the ways in which we specify knowledge and truth. Having previously set forth a notion of power as private and informal coercion that focuses on surveillance and its disciplinary consequences as opposed to traditional concepts of sovereignty, Foucault again seems to have presented a discursive framework that is well-suited to defining the Internet as a society.

Based on the lack of well-developed and formal governing laws, a discursive analysis of space and power online would focus on discipline that is more efficiently performed by other members of the online society as opposed to a governing body. Although it has been argued that many discourses are in conflict in any given struggle to label emerging behaviors online in terms of what behavior is deviant and what complies with the norm, it is an ad hoc disciplinary discourse within which the members of the Internet society determine legal and cultural societal norms. As states, corporations, and individuals struggle for power in cyberspace, some are concerned with the possibility that “governments and big business use the Internet to manipulate users and create a panopticon of intensified surveillance and control over society.”¹⁴⁹ Another commentator, Saskia Sassen, cites to a “de facto

---

²⁴³. Id.
²⁴⁴. Id. at 243-44 (citing the birth of the railroad as one example of a new technology).
²⁴⁶. Id. at 120-21.
management” of the Internet based on: (1) the roles of government agencies in technical standard-setting related to the software and hardware that make up the Internet, (2) increasingly large corporate interest in privatization of the Internet, and (3) the fact that the Internet Corporation of Assigned Names and Numbers (ICANN), a central authority, oversees key components of the operation of the Internet.50

While the law and corporate interests eventually might catch up with Internet society and overtake it, currently the more informal monitoring of online activity by individuals and corporate citizens drives the enforcement of Internet discipline. Through private litigation to enforce or determine existing regulations as well as communicative outlets such as press releases and social media tools, the Internet’s disciplinary discourse is driving its primitive society, at least for now.

III. ONLINE MEDIA AS THE PRINT CAPITALISM OF THE TWENTY-FIRST CENTURY

Benedict Anderson’s national communities were imaginable, he writes, due to the “explosive . . . interaction between a system of production and productive relations (capitalism), a technology of communication (print), and the fatality of human linguistic diversity.”51 He attributes much of nationalism to a fundamental change in people’s relationships to language, resulting from the mechanical reproduction and subsequent commoditization of print language in the 1500s when book publishers focused on profit and the market.52 According to Anderson, print capitalism expanded print markets beyond Latin, spread literacy, and brought a “change in the character of Latin itself.”53

Anderson proposes that print capitalism also resulted in an increased “fixity” to language.54 Anderson says that today’s language is more stable because we can access and understand the language of past centuries, something that was not possible before print capitalism.55 Finally, Anderson suggests that print capitalism resulted in hierarchies of languages-of-power that allowed some regions, communities, and ultimately nations to form a hierarchy of political dominance.56 This hierarchy of linguistic power, Anderson says, defines the relations of power and sets boundaries that might later be formed into nations with borders.57

Anderson has called print capitalism “the original mother of nationalism,” but he also has recognized the role of electronic media as being more powerful

51. IMAGINED COMMUNITIES, supra note 28, at 42-45.
52. Id. at 37.
53. Id. at 39.
54. Id. at 44.
55. Id. at 46.
56. Id. at 44-46.
57. IMAGINED COMMUNITIES, supra note 28, at 45.
than print, largely because it can instantly communicate images and symbols in different languages. He attributes new “long-distance nationalism,” characterized by dwindling dependence on territorial location, to the prevalence of simultaneous image and to migrations created by economic conditions. In her book, _Friction: An Ethnography of Global Connection_, Anna Lowenhaupt Tsing discusses Internet-based foreign investment as a forum for “dramatic performance” in support of economic opportunities. In Tsing’s example, a Canadian company, Bre-X, reported in 1997 a major gold strike in Indonesia, posting stories and prompting excited chat on their company website in support of the related investment opportunities. According to Tsing, one online commentator wrote of the Internet buzz surrounding the company, “The theater is open. The stage is set 24 hours a day. There is always an audience.” When the Bre-X hype proved to be baseless, and the gold strike an apparent fabrication, the economic effects on investors across the world and on Indonesia’s local economy were significant.

Through avenues such as Internet investing, online advertising, and public relations, the Internet is boundlessly extending the reach of the advantages and perils of global capitalism. In particular, tools of social media are becoming the most prevalent venues for online content sharing and creation worldwide. Widespread use of online social networking in conjunction with globalization has the potential to convert Anderson’s concept of long-distance nationalism into a newly imagined community in the style of print-capitalism, but with an even broader reach. Online member communities could foster a “postnational internationalism” that is inspired by and supports globalization.

IV. BEYOND NATION: IMAGINED COMMUNITY AND SOCIAL NETWORKING IN CYBERSPACE

Benedict Anderson portrays the idea of nation as imagined, primarily because we never meet or interact with the vast majority of other members of our nation. A postnational internationalism based on Internet communities would

59. Id. at 42.
60. ANNA LOWENHAUPT TSING, _FRICTION: AN ETHNOGRAPHY OF GLOBAL CONNECTIONS_ 56-57 (2005).
61. Id. at 65.
63. Id.
65. IMAGINED COMMUNITIES, _supra_ note 28, at 6 (arguing that nationalism with a capital N is hypothesized).
share this feature. According to Anderson, after the mediation through print capitalism of technical innovations between 1500 and 1800, “one could be fully aware of sharing a language and a religious faith . . . customs and traditions, without any great expectation of ever meeting one’s partners.”  

Increasingly, widespread communications and the standardization of languages through print capitalism allowed people to start participating in a common discourse and to imagine themselves as part of a larger community. However, Thomas Hylland Eriksen points out that we cannot take for granted “that people who identify with a given nation inhabit the same space, nor can it be assumed that cultural homogenisation takes place at the level of the nation though mass media.” The Internet, according to Eriksen, is “fast becoming a major medium for the consolidation, strengthening and definition of collective identities, especially in the absence of a firm territorial and institutional base.” The imagined communities of online partners who might never meet, like nationalism, brings people together. Online member communities also have the potential to create collective identities that draw from far more than shared geographical borders and institutional history. Although nation and nation-state might contribute to commonality among members of online communities, users of social media also have the opportunity to connect based on cultural affinities, interests, ideologies, philosophies, shared experiences and visions, or nearly anything at all. Social network communities based on caste affiliation in India, tenets of cross-border religious fundamentalism, and minority political views are a few examples of imagined communities that can come together online to foster connections in Internet society above-and-beyond those based on nationalism alone. In some cases such communities actually support ideas that run counter to the interests of nation.

From the perspective of participants in online member groups, many social networking options are available to allow individuals to connect with a particular member community within the cyberspace society. But the status of the social media field is changing rapidly. According to Gawker.com in 2009, the most popular social networking sites in the world were Facebook, MySpace, Orkut, hi5.com (leading in Peru, Colombia, Central America, Mongolia, Romania, and Tunisia, and others), Bebo and Skyblog (which, according to the website, “follow colonial patterns, the first strong in smaller English-speaking countries such as Ireland and New Zealand, and the latter in Francophone countries”), Friendster (which until recently led in Southeast Asia), and Fotolog (leading in

66. Id. at 188.


68. Id. at 5.
Argentina and Chile). 69 At the end of 2011, there were only seven markets where Facebook did not have the social media lead: Brazil, China (which blocks Facebook in substantial part), Japan, Poland, Russia, South Korea, and Vietnam. 70 While Facebook trails local favorites in these markets, it may be trending toward gaining the market lead, at least in Brazil. 71 Another change since 2009 has been the emergence of Twitter, which reaches at least one in ten Internet users worldwide, and ranks among the top social networks in 2012. 72 Twitter, which is known as a “microblogging” site because of its initial per-post character limit of 140 characters, grew at a rate of 59% in 2011 and continues to add users. 73 In Japan, Facebook is second to Twitter but is gaining users rapidly. 74

V. THE PHILIPPINES AS THE “SOCIAL NETWORKING CAPITAL OF THE WORLD”

A study released by Universal McCann in 2008 illustrates that 83% of the Philippines’ Internet users belonged to a social network at the time of the study. 75 A 2009 update of that study showed an increase in overall Internet use in the Philippines, 76 and a report in February 2010 showed that 90% of all Internet users in the Philippines visited a social networking site, making Filipino Internet users “the most engaged in social networking online.” 77 By 2011, the Philippines acquired the title of “Social Networking Capital of the World.” 78

Social networking in the Philippines has extended its reach to include an informational role in support of criminal investigations, 79 a role in the ability to connect and share information during a devastating flood in 2009, 80 and an

70. ComScore, supra note 4, at 8.
71. ComScore, supra note, at 8.
72. Id. at 10.
73. Id.
74. Id. at 9.
76. IMAGINED COMMUNITIES, supra note 28, at 6.
increasingly prominent role in election campaigns.\textsuperscript{81} While in the recent past political candidates have used the Internet to distribute campaign information, candidates can now use websites and social media to engage voters in dialogue. In addition, the May 10, 2010 presidential elections in the Philippines marked the first time that all voters in the Philippines cast their ballots electronically, a move attributed largely to “the sudden boom of social networking sites in the country.”\textsuperscript{82}

Long before the Asian financial crisis of the 1990s hit, the Philippines had its share of economic and social challenges. The Filipino history has had an undeniable bearing on its current willingness to adopt social media, although the extent of that bearing is difficult to quantify. Today’s Philippine democracy is predated by colonization under Spanish and United States rule, Japanese occupation, several elected presidents, and a dictator.\textsuperscript{83} Although it is seen as an independent democracy today, the Philippines has a challenging relationship with the concepts of nation and society.

The Philippines was colonized first by Spain during the fourteenth century, and later by the United States, beginning in 1898.\textsuperscript{84} As a former U.S. colony, the Philippines economy remained highly dependent on United States markets throughout the leadership of its five presidents between 1946 and 1965.\textsuperscript{85}

In 1965, Senate President Ferdinand Marcos won the presidency and many of his initiatives brought greater economic prosperity throughout his first term in office.\textsuperscript{86} He was re-elected as president in 1969, becoming the first president of the independent Philippines to achieve a second term.\textsuperscript{87} Unfortunately, economic growth declined during his second term, crime increased, there was growing public unrest, and also a threat of Communist insurgency.\textsuperscript{88} Marcos declared martial law in September of 1974, claiming that martial law was the prelude to creating a “New Society” based on new social and political values.\textsuperscript{89} Marcos officially lifted martial law on January 17, 1981, but retained much of the government’s power for arrest and detention.\textsuperscript{90} Regrettably, Marcos, his

\textsuperscript{81} \textit{Campaigns in Cyberspace}, MANILA BULLETIN (February 26, 2007, 8:00 AM), available at http://www.mb.com.ph/node/8594.


\textsuperscript{84} \textit{Id}.

\textsuperscript{85} \textit{Id}.

\textsuperscript{86} \textit{Id}.

\textsuperscript{87} \textit{Id}.

\textsuperscript{88} \textit{Id}.

\textsuperscript{89} \textit{Id}.

\textsuperscript{90} \textit{Id}.
wife, Imelda Romualdez-Marcos, and many of his top officials were accused of engaging in acts of corruption and economic self-interest.\footnote{Id.}

Marcos’s regime in the Philippines has been described as an authoritarian dictatorship, marked by “democratic formalities, bribes, patronage, control of the media and consolidation of bureaucratic power.”\footnote{See John Mark V. Tuazon, Mobile phones edge PCs in social network use: IDC, COMPUTERWORLD PHILIPPINES (Nov. 20, 2009), http://computerworld.com.ph/mobile-phones-edgepcs-in-social-network-use-idc.} Because of close ties between the United States and President Marcos, the U.S. government continued to support Marcos despite accusations of corruption and human rights abuses.\footnote{Id. at 1, 125.} Eventually, Marcos was ousted from the presidency in 1986 through a relatively peaceful “People Power Revolution.”\footnote{Id. at 1, 125.} The period since then, however, has been marked by political instability and slow economic productivity, having been hampered by the Asian financial crisis of the 1990s.\footnote{Tuano, supra note 17, at 3.}

Although it is impossible to know exactly why social media has become so popular in the Philippines today, its political history is surely a factor. In addition, a “friends-helping friends” culture, where friendship and favors might be “more valuable currency than money,” could also be credited with the rapid rise of social networking. Also, the ease with which users in the Philippines can access social media in a country with still-developing, region-wide Internet connectivity has been boosted by the increasingly cell phone-friendly format of social media sites. The prevalence of mobile phone use in much of the Asia-Pacific, including the Philippines, only allows for easier access to online networks. Users are able to bypass the need for Internet connectivity, directly connecting to friends and other online communities.\footnote{See John Mark V. Tuazon, Mobile phones edge PCs in social network use: IDC, COMPUTERWORLD PHILIPPINES (Nov. 20, 2009), http://computerworld.com.ph/mobile-phones-edgepcs-in-social-network-use-idc.}

VI. THE WARNET AND INDONESIAN TRENDS ONLINE

Although the Philippines is our world’s “Social Networking Capital” because it has the highest percentage of social media users based on its online population, Indonesia’s capital of Jakarta has the largest percentage of its online population using Facebook worldwide.\footnote{Jon Russell, Jakarta named world’s Facebook capital, ASIANCORRESPONDENT.COM (Mar. 18, 2011, 11:30 AM), http://asiancorrespondent.com/50592/jakarta-recognised-as-the-worlds-facebook-capital.} Online access in Indonesia has grown and continues to grow rapidly.\footnote{The Internet in Indonesia, 21 APSTER (Asia Pacific Network Information Center), Feb. 2007, at 1, 2, available at http://www.apnic.net/__data/assets/pdf_file/0010/27919/apster21-200702.pdf.} The Internet arrived in Indonesia in the early 1990s and initially was available only through universities and research
By the mid-1990s, however, Internet use began to play a larger role in Indonesian culture. In “The Internet, Social Networks, and Reform in Indonesia,” Merlyna Lim suggests that, although the Internet is still accessible to a relatively small percentage of the overall population, and instead of following Indonesia’s historical state and elitist domination over communication and media technologies, “the Internet was transformed into a new medium based on traditional network culture.”

Lim describes the overall rate of growth in numbers of Internet users as “explosive, even chaotic.” She attributes much of this growth to the advent of the Internet café, which is an extension of historical Indonesian culture. The term “warnet,” Indonesia’s term for an Internet café, combines the Indonesian term warung, a casual meeting place where non-elite members of Indonesian society gather to eat and commune, with the Internet. Based on its amalgamation of the new digital media that the Internet brings with the centuries-old tradition of the warung, the warnet, according to Lim, is “culturally entrenched in Indonesia’s traditional social network formation” and is a key focus of Indonesian culture, both as a neighborhood meeting space and a micro-civic community that replaces the traditional warung in the lives of many.

In Engineers of Happy Land: Technology and Nationalism in a Colony, Rudolf Mrazek previews his book’s discussion of technology in Indonesia’s late Dutch-colonial culture by framing new technologies of pre-1942 Indonesia:

Encountering the “unseemly” technologies, people in the Indies often began to move, speak, and write in a way that broke through – or at least scratched – the otherwise smooth surface of their behavior and language. While the people handled, or were handled by, the new technologies, their time, space, culture, identity, and nation came to feel awry.
Perhaps Mrazek’s assessment of new technologies of late-colonial Indonesia presents an apt articulation of the possible link between the rise of the warnet and a 1998 uprising in Indonesia more than fifty years later.

General Suharto took over the presidency in Indonesia after a failed communist coup in the mid-1960s, bringing what he called a “New Order” of anti-communism, strong military involvement in government, and a pledge to tenaciously promote economic development.107 Anna Lowenhaupt Tsing says that “the New Order regime of General Suharto (1966-1998) made business a predator, born from the mix of nepotism, international finance, and military muscle, and feeding on cheap resources ripped illegally from rural communities.”108 Eventually, Suharto was forced to resign from the presidency in the midst of the Asian financial crisis that began in 1997 as the Indonesian economy was crashing, stepping down on May 21, 1998, after mass demonstrations and student uprisings in which 500 people were killed.109

In a 2004 article, Merlyna Lim proposed that warnet use throughout Indonesia fostered the building of individual identities that were subverted by the Suharto government in favor of a uniform state identity.110 Beginning with the warnet culture in the mid-1990s, individuals were more easily able to connect with alternative information, ideas, and political parties through websites.111 These connections, according to Lim, potentially aided the process of democratization in Indonesia that began with the forced resignation of authoritarian leader General Suharto in 1998.112 Rather than their identities feeling “awry,” in Mrazek’s words, as the result of the growing Internet technology,113 it is possible that many of the participants in the 1998 political revolution, particularly members of the student movement, found through the new technology of the Internet the ability to re-create a political identity separate from that of the “New Order” state of authoritarian leader General Suharto. Perhaps it was the advent of the technology that allowed Internet-users to understand that their identity and nationalism under the New Order were awry, with the Internet serving as a possible a path to a more suitable order.

Although approximately 2% of Indonesians use Facebook today, use continues to trend upward.114 Lim is confident that against the backdrop of the cultural exchange meeting space of the warnet, “the Internet has become a novel

---

108. Tsing, supra note 60, at ix.
110. Polarization of Identity, supra note 49.
111. Id.
112. Id.
113. Mrazek, supra note 106.
space for information exchange,” which has led to more open political discourse, public access to information, and a more democratic Indonesian society.

The current president of Indonesia apparently agrees. During the summer of 2011, Indonesian President Susilo Bambang Yudhoyono encouraged attendees at a meeting for the Association of Southeast Asian Nations (ASEAN) to capitalize on the opportunity to engage with citizens through social media outlets such as Facebook and Twitter. Facebook recently passed the Indonesian version of Google as the most popular social networking site with 15.8% of the population participating. Indonesia’s rate of adoption of Facebook is second only to that of the United States, and in a country in which only approximately 16% of the population uses the Internet, compared with about 77% in the US, Facebook’s Indonesian penetration rate is impressive. And President Yudhoyono wants social media to continue to thrive across Southeast Asia, because he very well may see the cues to the future economic stability of his country in Indonesia’s history with the Internet.

Coincidental to Internet adoption or not, Indonesia’s financial growth is also currently rapid. Foreign investment in Indonesia increased 52% to $16.2 billion between 2009 and 2010. Although the country’s financial stability is susceptible to fluctuation, Indonesia looks to be moving in its desired direction and President Yudhoyono appears to recognize the potentially significant contribution of the Internet and social media in the process, as evidenced by his encouragement of all ASEAN nations to join Indonesia in continuing to increase Southeast Asia’s presence in the online community.

VII. THE FACE OF CONTEMPORARY GLOBALIZATION

During the last two decades of the nineteenth century, the telegraph, transoceanic cables, increasing efficiency of mail delivery, and railway expansion were highlights of the era Benedict Anderson calls “The Age of Early Globalization.” Ever-increasing movement of people, languages, and ideas across physical borders strengthened the intercontinental networks that form the

115. Lim, supra note 101, at 283.
119. AFP, supra note 116.
121. Id.
122. AFP, supra note 116.
123. BENEDICT ANDERSON, UNDER THREE FLAGS 233 (2007).
basis of what we know as globalization today.\textsuperscript{124} Between early and
contemporary globalization is a history of war, struggles with colonization, and
more technology than could possibly have been contemplated at the turn of the
nineteenth century.

The Internet certainly is one of the transformative, unanticipated
technologies that continues to have a direct impact on globalization. Merlyna
Lim refers to the “anarchic characteristic” of the Internet and articulates that this
type of technology had wide-ranging effects.\textsuperscript{125} Lim says that:

\begin{quote}
The relation between technology and society ranges far beyond the
causal relationship between the technology and its immediate users.
Rather, the interconnection between technology and society is
historically and culturally rooted in a local context, which is the nexus
where technology and society meet, and on the basis of which
technology’s impact spreads widely through society.\textsuperscript{126}
\end{quote}

Of course, Internet society and the technologies that support it are inextricably
linked. Perhaps it is through the Internet society that this interconnection leads
to a “new” globalization, one that represents both a quantitative and qualitative
shift in the face of the globalized world.

Quantitatively, neoliberal economics and a more integrated economy based
on global trade have resulted in a new basis for economic power. In
Globalization and Sovereignty, John Agnew finds that, “the globalizing world
economy is not an economy of national territories that trade with one another,
notwithstanding the tendency of the World Bank and other international
organizations to portray it this way.”\textsuperscript{127} Instead, Agnew says, the globalized
economy acts as a “complex mosaic of inter-linked global city-regions,
prosperous rural areas, resource sites, and ‘dead lands’ increasingly cut off from
the technologies of time-space compression that fuel globalization.”\textsuperscript{128} Agnew’s
point aptly demonstrates the economic shift methodically wrought by
capitalism’s global drive.

Qualitatively, the social, cultural, and political backdrop of globalization
should not be discounted. Lim’s previously stated notion that “interconnection
between technology and society is historically and culturally rooted in a local
context” can explain the popularity and continuing growth of Facebook.\textsuperscript{129} As
growing Facebook adopters with rich colonial and authoritarian histories,
residents of Indonesia and the Philippines face critical issues related to
nationalism and emerging technology that are likely representative of much of
the developing world. In the Philippines, perhaps it is the culture of connection

\textsuperscript{124} Id. at 233-34.
\textsuperscript{125} Lim, supra note 101, at 274.
\textsuperscript{126} Lim, supra note 101, at 274.
\textsuperscript{127} JOHN AGNEW, GLOBALIZATION AND SOVEREIGNTY 213-14 (2009).
\textsuperscript{128} Id. at 214.
\textsuperscript{129} Lim, supra note 101, at 274.
and dependence on friends that feeds the growth of social network activity. In Indonesia, the adaptation of the warung into a warnet is the local cultural context that has likely driven its rapidly growing popularity there.

Leading the social media field in the Philippines and rapidly taking over in Indonesia, Facebook hosts the largest network of individuals worldwide at over 600 million users and growing.\(^{130}\) In addition to allowing citizens of the Internet Society to connect with each other and share information, ideas, and advertising, Facebook’s terms of use include the assurance that, “[w]e strive to create a global community with consistent standards for everyone, but we also strive to respect local laws.”\(^{131}\) Recognizing its global audience, Facebook administrators, still led by the network’s founder and CEO, Mark Zuckerberg, continue to expand the reach and ability of all users to make connections.\(^{132}\) In April 2011, a marketplace for private company trading estimated that Facebook’s value was $80 billion, up from $11.5 billion in 2010, a fact that caused speculation about the possibility of a public offering in Facebook’s future.\(^{133}\) Facebook’s IPO was predicted to be the biggest public offering of 2012, and in May it did not disappoint, becoming the largest tech IPO in U.S. history, raising $16.1 billion.\(^{134}\)

Today’s Facebook offers myriad implications for globalization fueled by its online member communities. Facebook’s privacy policy, which can and has been changed frequently, sets forth some of the information that is collected by Facebook from its users.\(^{135}\) For example, the software keeps track of many user actions on Facebook, such as “the information you choose to share when you take an action, such as when you add a friend, like a Page or a website, tag a place in your post, find friends using our contact importers, or indicate you are in a relationship.”\(^{136}\) In addition, user location information is collected based on mobile phone use and the computer’s IP address.\(^{137}\) The software also collects information from third party applications that users access through Facebook, including information from them.\(^{138}\) The Facebook privacy policy states that

---

\(^{130}\) IMAGINED Communities, supra note 65, at 20-24.
\(^{136}\) Id.
\(^{137}\) Id.
\(^{138}\) Id.
“[w]e use the information we receive about you in connection with the services and features we provide to you and other users like your friends, the advertisers that purchase ads on the site, and the developers that build the games, applications, and websites you use.”139

In terms of the global market-related information collected from hundreds of millions of users, the Facebook privacy policy also states that:

For example, we may use the information we receive about you:
[1] to measure or understand the effectiveness of ads you and others see;
[2] to make suggestions to you and other users on Facebook, such as: suggesting that your friend use our contact importer because you found friends using it, suggesting that another user add you as a friend because the user imported the same email address as you did, or suggesting that your friend tag you in a picture they have uploaded with you in it.

Advertisers also may choose the characteristics of users who will see their advertisements, fed by “non-personally identifiable attributes we have collected (including information you may have decided not to show to other users, such as your birth year or other sensitive personal information or preferences) to select the appropriate audience for those advertisements.”141

Under Facebook’s current privacy policy, users may opt out of many of the information-sharing features of Facebook.142 However, the possibility that Facebook will change the policy makes it difficult to know what this access to global market information will look like, even in the near future. As it stands, Facebook can let a business user know quite a bit about where someone is located, what many of his or her interests might be, the members of his or her online community, and also something about his or her actions and activity online.143 Members of online communities linked to social networks, using Facebook as the largest example, are members of definable, traceable communities within the Internet society. These online member communities, while not mutually exclusive of nations, are supplanting Benedict Anderson’s version of nation-building with community-building based on members’ places in a global Internet society as opposed to a territorialized nation-state.

139. Id.
141. Id.
142. Id.
143. Id.
A. PII, Behavioral Targeting and Privacy

From a business standpoint, it is valuable to know as much as possible about a consumer and what he or she is seeking. As technology progresses, the process of researching consumer behavior is becoming increasingly accurate and efficient in every way. Although the practice of tracking a consumer’s online activities over time has been possible since at least the early 1990s with the advent of the World Wide Web, the level of sophistication of tracking technologies has risen precipitously. Website applications and device identification tools that send information to external sites are becoming more common results of website visits from a computer or a cellular phone. Basic “cookie” technology – the downloading of a small text file (the cookie) onto a website visitor’s computer for the purpose of identifying that user on future visits – has been widely used since the early 1990s. As web cookies and other tracking capabilities have evolved, businesses are able to collect or purchase information about the various websites a user frequents, the length of time spent on each site, the user’s interactions with the sites, keywords, or comments that the user enters on the sites, as well as types of purchases that the user makes. Detailed user profiles are available for businesses so that they can determine the optimal advertising to display to a particular user, depending on the online behavior of that user. This “behavioral advertising” has become more controversial as data re-sellers and advertising interests collect more and more information.

Historically, web cookies have been used to store information about a website user, including login information, website navigation activities, the content of an online shopping cart, or website customization preferences. Cookies can be dropped onto a computer hard drive or embedded in the user’s Internet browser by a website, or by a third party vendor affiliated with the website, such as an online advertising company. A traditional cookie will remain active until it is deleted or expires. Information from the cookie is stored in a log file under the user’s computer IP address or under an assigned

146. Id.
147. Id.
148. Davis, supra note 144.
149. Id.
150. Cookies were commonly set to expire in 2038, but recently companies have reset most expiration times to 2 years, amid growing consumer concerns. See, Linda Rosene, Google: User Cookies to Expire After Two Years, PC WORLD ONLINE (July 17, 2007, 2:00 PM), http://www.pcworld.com/article/134669/google_user_cookies_to_expire_after_two_years.html.
identification number.\textsuperscript{151} As a user continues to navigate the Internet, whoever dropped the cookie will generally be able to analyze all of the sites the user has visited and what the user did on these sites to create a very detailed profile.

Businesses tend to characterize the data collected by cookies as “anonymous” as opposed to “personally identifiable” information (PII), regardless of the accuracy of that label under any given applicable law.\textsuperscript{152} The aggregation of this anonymous information has great commercial value and can be sold to businesses interested in online market trends. As website users became more aware of the tracking activities of cookies and understood that they could delete them, behavioral tracking moved into a realm of “Flash cookies,” based in Adobe’s Flash Player, that do not expire, can store more information than traditional cookies, and are stored in a different location on the user’s computer thereby becoming more difficult to delete.\textsuperscript{153} Since public awareness and concern about these hardy cookies has grown, more recent versions of Adobe’s Flash player were developed to be compatible with a computer or mobile phone’s browser settings, so if a user chooses to temporarily store cookies and delete them at the end of a browsing session, that election will apply to Flash cookies as well.\textsuperscript{154} Flash cookies also can be used on mobile devices that support Adobe’s Flash technology.\textsuperscript{155}

Additional tracking technologies used in combination with cookies are “web bugs,” which also are known as web beacons, tracking bugs, tracking pixels, pixel tags, cookie anchors, or clear gifs.\textsuperscript{156} A web bug is a tiny, generally transparent, graphic image that is placed on a website or in an e-mail that is used to monitor the behavior of the website or e-mail user.\textsuperscript{157} The web bug is hosted on an external site, its code points to a site to retrieve that image, and at the same time it can send information to the site that hosts it, including the IP address of the computer that is displaying the image.\textsuperscript{158} The web bug also can associate the computer’s user with an active cookie that resides there, so whoever hosts the web bug can track the user and profile of that user’s browsing behavior. Web

\begin{enumerate}
\item\textsuperscript{151} Angwin, \textit{supra} note 145.
\item\textsuperscript{152} Angwin, \textit{supra} note 145.
\item\textsuperscript{153} Flash cookies can also be used to recreate cookies that a user has deleted though a process known as “respawning.” See, Jeremy Kirk, \textit{Study: Adobe Flash Cookies Pose Vexing Privacy Questions}, \textit{PC World Online} (August 11, 2009, 9:20 AM), http://www.pcworld.com/article/169985/study_adobe_flash_cookies_pose_vexing_privacy_questions. Flash cookies are the subject of at least three lawsuits in the United States, which allege that tracking companies that used them violated computer security and privacy laws.
\item\textsuperscript{154} Id.
\item\textsuperscript{155} Id.
\item\textsuperscript{156} Angwin, \textit{supra} note 145; \textit{see also Web Beacons and Other Tools}, \textit{AllAboutCookies.com}, http://www.allaboutcookies.org/web-beacons/index.html (last visited Jan. 20, 2012).
\item\textsuperscript{157} Angwin, \textit{supra} note 145.
\item\textsuperscript{158} Id.
bugs generally are invisible and cannot be deleted, as they are stored on a external server.\textsuperscript{159}

Tracking through geolocation technologies also is becoming extremely prevalent in Internet use through computers and mobile phones.\textsuperscript{160} These technologies are often used by mobile phone applications and social networking websites to determine the geographical location of the Internet user.\textsuperscript{161} A user’s location can be determined by a number of different technologies, including Global Positioning Satellite (“GPS”), Wi-Fi positioning, and IP address location.\textsuperscript{162} Geolocation technologies can be used for a wide range of purposes, such as criminal activity detection, location authentication, security and network efficiency, and, of course, targeted advertising.

Deep packet inspection (“DPI”) is another technology used by Internet service providers to monitor, track, and record the online and mobile activities of their users.\textsuperscript{163} When information is transmitted over the Internet, it is broken down into packets, routed to its destination, and reassembled into the original content.\textsuperscript{164} DPI allows the examination of these packets of information.\textsuperscript{165} DPI technology can be used to develop accurate user profiles, as it can access any unencrypted information transmitted or received by the user.\textsuperscript{166}

Reverse-engineering the information that is sent out based on tracking technologies to pinpoint an Internet user can be quite accurate. For example, when Netflix released anonymous movie rankings by its customers in 2007, researchers from the University of Texas were able to positively identify customers by combining the Netflix data with publicly available information found elsewhere online.\textsuperscript{167} The same thing was done by researchers when AOL released what they classified as anonymous data comprised of twenty million web search queries.\textsuperscript{168} With the actual anonymity of tracked information in

\textsuperscript{159} Id.

\textsuperscript{160} Daniel Ionescu, Geolocation 101: How it Works, the Apps, and Your Privacy, PCWORLD.COM (Mar. 29, 2010, 10:45 PM), http://www.pcworld.com/article/192803/geolocation_101_how_it_works_the_apps_and_your_privacy.html.

\textsuperscript{161} Id.

\textsuperscript{162} Id.

\textsuperscript{163} M. Chris Riley and Ben Scott, Deep Packet Inspection: The End of the Internet as We Know It?, FREEPRESS.NET (Mar. 2009), http://www.freepress.net/files/Deep_Packet_Inspection_The_End_of_the_Internet_As_We_Know_It.pdf (last visited Jan. 10, 2012).

\textsuperscript{164} Id.


\textsuperscript{168} Id.
question, privacy regulation regarding the collection, use, and sale of that information becomes much more important economically as well as socially.

B. PII, Privatization and Commerce

Online tracking of individuals is becoming more common and more pervasive. Most commercial websites download some form of tracking software onto users’ computers, from cookies to recall user names and passwords to, more commonly, up to hundreds of files or programs being downloaded onto a computer by one website, most of which typically originate from companies that track and sell web user data.169 Many of these tracking files can predict a website visitor’s age, gender, and ZIP code, and may also contain a code that generates an estimate of income, marital status, number of children, and home ownership status.170 The resulting tracked information might be considered “anonymous” by most standards, as it identifies web users by a number assigned to their computer, not their name, U.S. social security number, or other personal data.171

The presence of tracking programs is not always apparent to an Internet user. These programs often come from hidden files within downloads or display ads.172 Certainly, consumers might appreciate the personalized experience that is made possible through a third party comprehensively tracking Internet behavior; however, relevant and targeted ads are just one result of online data collection. This type of data is a significant source of revenue for web-based companies,173 and it stands to gain in net worth as more interested parties discover the value of collected information and are willing to pay for it.

Internet tracking technologies make extremely valuable commercial data available, potentially to the highest bidder.174 The owner of this data can use it to market goods and services as well as politics and ideologies.175 This valuable data can be seen as a new form of capital within the Internet society, capital that potentially has great significance to the global economy. The manner in which an individual or a larger audience is targeted through marketing based on Internet behavioral tracking can affect the way diverse groups of people perceive and interact with each other. More specifically, information tracking technology and the capital it spawns have a direct impact on the power and autonomy of consumers and all Internet users.

169. Researchers at AT&T Labs found tracking technology on 80% of 1,000 popular websites, up from 40% of those sites in 2005. See Angwin, supra note 145.
170. Id.
171. Id.
172. Id.
173. Id.
174. Id.
175. Angwin, supra note 145.
VIII. POST-CRISIS SOCIAL NETWORKING AND POST-NATIONAL INTERNATIONALISM

In 1980, Gilles Deleuze and Félix Guattari stated:

Today we can depict an enormous, so-called stateless, monetary mass that circulates through foreign exchange and across borders, eluding control by the States, forming a multinational ecumenical organization, constituting a de facto supranational power untouched by government decisions. But whatever dimensions or quantities this may have assumed today, capitalism has from the beginning mobilized a force of deterritorialization infinitely surpassed by the deterritorialization proper to the State.\textsuperscript{176}

More than twenty-five years later, Saskia Sassen supported the concept that economic globalization has resulted in deterritorialization and an overall decline in the importance of the state.\textsuperscript{177} Sassen also has commented on the denationalization of former national state agendas, which now fall into the realm of global capital in a global market, despite their continued characterization as “national.”\textsuperscript{178}

In \textit{Cities in a World Economy}, Sassen discusses “a new phase of the world economy” that began with the collapse in the 1970s of the United States’ political, economic, and military dominance and also the reentry of Western Europe and Japan into international markets, which was strengthened by the Asian financial crisis in the 1990s.\textsuperscript{179} More recently, Sassen has proposed that the concepts of “national territory” and “state authority” take on different meanings in the new global economy.\textsuperscript{180} John Agnew cites to North America, Europe, and an economically-improving East Asia as the significant “anchors” of the new global economy.\textsuperscript{181} “The new globalization represents the first impact of the global on a previously state-centered world,” according to Agnew.\textsuperscript{182} It seems that the both Sassen and Agnew agree that “nation,” and by analogy nationalism, no longer exist as they did under systems based more wholly on state sovereignty, or at the very least they operate under the new set of rules that the new globalization has unveiled.

In discussing New Order Indonesia, Anna Lowenhaupt Tsing proposes that “Nationalism lost its promise, as imperially mandated authoritarian rule came to
define the Third World.”183 Although she admits that many scholars would treat the concept of nation as a “worn shoe discarded in the race toward globalization,” Tsing cites to the continuing relevance of nation as crucial to political struggle.184 With regard to the Philippines, Albert Celoza says that “since the latter nineteenth century, nationalism has been important to Philippine history, but even up to the present time, it remains a weak force compared to the hold of ethnicity and patron-client relationships.”185 He goes on to say the following:

In a nation where nationalism and ideology are still developing, authority and obedience can be established by giving and withholding tangible rewards and by threatening to use force or punishment; thus Philippine history and society have been molded by allegiances to the nation and to the group. More often than not, the latter prevails, and at certain times the prevalence has not been beneficial to national interests.186

The “allegiance to group” that marks Philippine history seems relevant to postcolonial, post-authoritarian Indonesian society as well. In both states, this allegiance fosters the postnational internationalism in support of globalization that is made possible through access to online communities. The online communities might prove to be the groups that are most relevant to social, political, and economic development in Indonesia and the Philippines, as well as across the globe. Therefore, the consequences to the long-term well-being of the world economy because of proposed online regulations are myriad. Social and economic capital created by online networking and associated datamining could continue to change the face of the global economy in any of a number of directions.

IX. CONCLUSION

The process of individuals in Indonesia and the Philippines embracing Internet technology and, likely by default, its postnational implications are representative of the drive within Internet society in support of a qualitative and related quantitative shift in the face of globalization. In light of the growth of the Internet society and the wide adoption of social media across geographical boundaries, nation-building is being supplanted by online community-building. Tools of social media are becoming the most prevalent venues for online content sharing and creation worldwide. Both the manner in which online social interaction of individuals and groups is targeted through behavioral tracking and use of resulting data that is mined through tracking ultimately can affect the way

183. TSING, supra note 60, at 84.
184. Id. at 84-85.
185. CELOZA, supra note 85, at 9.
186. Id. at 9-10.
diverse groups of people perceive and interact with each other. Behavioral tracking online also has economic ramifications based on the end-use of mined data. As the enormous financial incentives to gain control of the globalized Internet society and its goldmine of data become obvious, the attempts at regulation and laws that control the environment become at the same time critical and overwhelming.

In lieu of blindly welcoming as inevitable the postnational capital sustained by the new globalization, it is crucial to consider the implications of the increasingly sweeping inclusiveness of the Internet society. While socio-economic factors make online access and participation far from comprehensive, the number of individuals globally who are online is dramatic. Even more striking is the potential for harnessing and exploiting the millions of members of Internet society and a majority of the globalized world by unchecked forces of globalization in the hands of private interests. Before Facebook and the many other Internet connectors and collectors of individual statistics and valuable market data fall significantly into private ownership, the ramifications of this new form of capital on the global market should be considered. Whether backed by national currencies or golden mined data, capital concentrated in the hands of the wrong stakeholder(s) can sink an economy. The postnational global market, as supported by Internet society, might very well be the single most important market to watch in terms of the long-term economic well-being of the world economy. As governments and private interest groups struggle with the appropriate level and form of regulation addressing the Internet, they hopefully are mindful of the extremely high stakes.
PRIVACY AND CONFIDENTIALITY ISSUES IN HISTORICAL HEALTH SCIENCES COLLECTIONS

Anne T. Gilliland* and Judith A. Wiener**

I. INTRODUCTION

Historical health sciences collections are rare and unique materials containing large amounts of information subject to confidentiality and privacy laws and concerns. Formerly, the custodians of these collections handled these issues in relative obscurity, but technological changes and changing laws and norms around health care privacy have made these issues more acute and public. The intent of this Article is to describe the nature of these collections and the qualifications of the people who administer them, and to analyze some of the privacy and confidentiality issues that arise in the course of that work. The aim is to acquaint privacy officers, in-house legal counsel, and other members of the legal profession with the privacy and confidentiality challenges that these collections present, with the needs of researchers who use these collections, and with the reasons why historical health sciences collections are important.

Part II will discuss the nature of historical health sciences materials and of the people who work with these collections.1 In Part III the authors identify privacy and confidentiality laws and circumstances that affect these collections with a special emphasis on the Health Insurance Portability and Accountability Act (HIPAA).2 Part IV discusses strategies and solutions for complying with these laws and circumstances while still providing access to researchers and protecting the integrity of the historical record.3

II. HISTORICAL HEALTH SCIENCES SPECIAL COLLECTIONS

Health sciences libraries of every scope and size, from modest community hospitals to academic medical centers, often have historical or special collections of some quantity within their holdings. These materials come into a library through a variety of methods and can be comprised of a multitude of formats. The assorted provenance of the materials combined with the wide variety of

---

* Anne T. Gilliland, J.D., M.S.L.I.S., is the Scholarly Communications Officer for the Libraries at the University of North Carolina, Chapel Hill.
** Judith A. Wiener, M.A., M.L.I.S., is Assistant Professor and Assistant Director for Special Collections and Outreach at the Health Sciences Library at the Ohio State University.
1. See discussion infra Part II.
2. See discussion infra Part III.
3. See discussion infra Part IV.
formats often makes these collections susceptible to privacy concerns and subject to privacy and confidentiality laws.4

Historical health sciences collections materials differ from general patient records within a medical environment because they are believed to have enduring historical or other value that can differ from the purpose for which they were created.5 In a chapter in the book, Capturing Nursing History, Keith C. Mages and Julia A. Fairman give the example of the ward diary of Mary Clymer, a student nurse in the 1880s, and the “vivid glimpse into the past” that this sort of primary source in a historical health sciences collection can offer.6 Accounting books that doctors created at the beginning of the 20th century to document patient accounts can be used by historians to study the economics of health care during the time period. Likewise, films created to instruct nurses in best care practices can be studied to trace the history and evolution of women’s professional roles by gender study researchers.

A. General Role and Scope

1. Types of Collections

According to the Association of Research Libraries, the term “‘special collections’ has been used in North American libraries in many different ways.”7 Most commonly it refers to rare books, manuscripts, archival collections of mixed formats and printed materials, such as newspapers and pamphlets not held in book form.8 As technology develops and information delivery methods evolve, so does the nature of these collections, such that it is now common to find that materials such as audio visual and digital material have been added to the umbrella of special collections departments.9 A common thread in the variety of materials within such departments is that they are rare or unique. In addition, they often fall within a particular collection scope, such as a regional or subject specialization.

8. Id. at 5-6.
9. Id. at 6.
2. Types of Materials

Special collections repositories in the health sciences often contain the same types of textual and non-textual materials listed above. Depending on the type and breadth of the collections, the materials may contain privacy-sensitive materials. Historically, the protection of sensitive health care information was entrusted to the care and custody of one’s physician. Professional physician codes of ethics focusing on the patient’s privacy right were established early and can be found within the Hippocratic Oath. In general, patients entrusted their physicians to act on behalf of their best interest in regards to privacy, and physicians were expected to uphold this expectation in their interactions with their patients. Absent the establishment of privacy legislation, the amount and type of information that could be documented, shared or saved was left to the physician’s or health organization’s best discretion.

Physicians and medical organizations often turned records from their daily practices over to special collections or archival areas of libraries as the materials aged and were not needed on a daily basis. Commonly, donors recognized the records’ historical or documentary value. As a result, the degree of privacy-sensitive information contained within medical archives can vary widely within any given institution. This information can include detailed information about patient health contained in a physician’s journal, correspondence between a patient and health care provider, detailed logbooks kept by hospitals, or detailed photographs of patients or research subjects. In many cases in the past, custodians may not have paid careful attention as to whether or not privacy-sensitive material was located within their collections because privacy laws were less stringent and because of the sheer volume of material that they collected.

3. Common Institutional Affiliations and Staffing

Staffing patterns vary among special collections units within health care organizations. Large academic medical centers commonly have professionally-trained curators or archivists who staff special collections departments within hospitals or health sciences libraries, while smaller hospitals may have a less formal department, such as a storage room supervised by an administrative professional or volunteers.

10. See generally Gilliland supra note 4.
Professionally trained curators or archivists are likely to possess master’s degrees granted by history or library science programs. These individuals usually employ a standard archival arrangement and description theory that emphasizes the higher organizational level of collections, rather than detailing materials at an individual level. Normally, archives are arranged at a collection level to preserve the organization given to it by the creator, in order to preserve the original documentary relationships and as a way to organize the mass volume of modern records efficiently. For example, letters are often described in an archival inventory, or finding aid, as a group under the subject of “correspondence,” rather than listed or described by their content individually. Archival theory emphasizes that materials should be kept in the same original order that their creator maintained them, so in many cases, when collections come into an archival facility in reasonable order, archival staff keep documents in that same order without item-level examination. Therefore, a great deal of private information may be present within collections without the knowledge or intellectual control of anyone at the institution.

B. Traditional Confidentiality and Privacy Concerns and Methods for Resolving Them

1. Privacy and Confidentiality through Obscurity

Prior to the development of the Internet and technology for digitization, the risk for widespread exposure of privacy sensitive archival materials was more limited. The rare and unique nature of the material contained within special collections means that they are often not physically circulated or available for checkout by library patrons. Often a researcher would have to travel to the archives and go through archival materials on-site in order to physically view them. Today, although researchers still visit reading rooms, more and more materials are available online or provided in digitized form. Online publication of finding aids has facilitated discovery of materials in historical health sciences collections and increased demand for digitized content.

2. Access Control in the Reading Room

When researchers visit a reading room, often they must provide identification, sign release and use forms that document they understand the

15. Miller, supra note 5, at 19, 28-30.
17. Miller, supra note 5, at 20, 31, 37-41.
18. See generally TRINKAUS-RANDALL, supra note 14; see also Gilliland, supra note 4, at 391-92.
rules and policies of the particular archival institution, and leave their belongings, except for pencils, and some paper or perhaps a laptop (if permitted), outside the reading room area. Typically, custodians pull material and artifacts from closed stacks for researchers to consult, usually a box at a time. Materials may not leave the secure reading room environment of the library, and copying of materials is limited because of security, theft, handling, and preservation concerns. In addition to providing for the protection and preservation of rare and sometimes fragile materials, indirectly, these policies also protect privacy and confidentially through obscurity and barriers to access on-site. Although on-site researchers have access to privacy-sensitive records and materials, the risk of widespread breach of any confidence or privacy issues is limited because the records are not shared widely beyond the confines of the reading room.

C. Contemporary Confidentiality and Privacy Issues

1. Role of the Internet and Digitization

The advent and increased use of technological means to promote and increase access to special collections materials has exponentially increased the threat of widespread confidentiality and privacy breaches to users. In the past, only one researcher at a time could access a limited amount of material in an archival reading room, but today, archival digitization and discovery projects have created an environment where anyone can access special collections materials anywhere, at any time, and for any purpose. Digitization is a great tool for increasing access to rare or unique materials and promoting the use of archival materials. At the same time, this widespread access has serious implications for the protection of privacy of those individuals whose lives and medical information may be reflected within the collections. This, in turn, places an organization at greater risk for HIPAA and other privacy legislation violations, especially if these digitized holdings are made available through widespread Internet discovery means, such as search engines or digital libraries.

2. Changing Norms for Donor Agreements and Expectations

The ability of technology to make records available for widespread distribution and access may also pose risks to donation agreements and donor

22. Gilliland, supra note 4, at 392.
expectations. Donors who felt comfortable with the mission and archival access policies of a special collections unit may have given material with few or no restrictions. These same donors might have felt quite differently about their entrustment if they had known, or could have imagined, that the materials given to document or preserve the historical record in one setting would one day be made openly accessible to a wide audience without restriction of use or purpose. Compounding this issue is the fact that older donor agreements and contracts may not have addressed digital distribution methods, even when they were possible, or that the donors of such materials may not have had the rights or permission to provide such access. When feasible, some donor agreements may need to be revised or revisited.

3. Beyond Privacy and Confidentiality Law—Ethical Concerns in Historical Health Sciences Collections

The archival professional is bound by a set of ethical standards that encourages him or her to maintain a careful balance between providing wide access to materials while protecting the privacy of those who are documented within the materials. The major professional organizations that maintain the local and global standards and expectations of their members all include language within their codes of ethics that speak to these seemingly contradictory responsibilities and dictate that the privacy of the individuals reflected within archival materials should be protected and weighed against the professional duty to provide access to materials. Thus, the use restrictions and access structure solutions provided by HIPAA may provide archivists with the opportunity to develop a structure and solution to the problem of balancing access against privacy in accordance with the law and their own professional ethical standards.

24. Gilliland, supra note 4, at 392.
25. Gilliland, supra note 4, at 392.
III. CONTEMPORARY PRIVACY AND CONFIDENTIALITY LAWS AND CIRCUMSTANCES THAT AFFECT HISTORICAL HEALTH SCIENCES SPECIAL COLLECTIONS

Although historical health sciences special collections custodians have long been concerned about privacy and confidentiality issues with regard to their collections, several laws and trends have made these issues more urgent. The foremost concern is the Health Insurance Portability and Accountability Act (HIPAA). Other Federal statutes, as well as state privacy and confidentiality laws, also may apply to certain collections or parts of collections. In addition, there are changing expectations around privacy from the donors or potential donors, from the subjects of the historical health sciences special collections (when they are living or from their heirs), from the scholars who do research in these collections, and from the institutional boards that regulate and oversee this research.

A. Health Insurance Portability and Accountability Act

HIPAA has preempted many state laws for breach of privacy and breach of confidence. Although HIPAA was not aimed specifically at the historical health sciences special collections community, its effect on these collections has been substantial. Traditionally, archival professionals relied on their own best professional judgment, tied to their system of professional ethics to provide access to sensitive materials. This approach was a careful balance of providing access while maintaining privacy. HIPAA, however, overrode this long-established professional judgment system as organizations became concerned about how to apply the law to collections that fell under HIPAA but were not the focus of the law. Confusion ensued as archival leaders sought direction from their internal counsel and even Congress and were provided with uneven responses to their request for resources. In many cases, responses to researchers and to collections custodians have been contradictory or incomplete.

31. Id.
33. See generally Gilliland, supra note 4. See also Wiener, supra note 32, at 16-18.
36. See generally Lawrence, supra note 35.
37. Lawrence, supra note 35, at 423.
1. Purpose of HIPAA

Congress passed HIPAA in 1996 which forced the federal government to address issues of privacy and confidentiality in an age where technology made the exchange of health information easier.\(^{38}\) The two primary concerns were to enable electronic exchange of health information by providing sufficient security constraints and to secure health information that might come to light as preexisting conditions when workers changed jobs.\(^{39}\) Consequently, HIPAA applies to certain types of health care organizations that transmit information electronically.\(^{40}\)

Although the purpose of HIPAA was not directly related to historical health sciences special collections, legislators were aware that its provisions would have an impact on these collections early on.\(^{41}\) As regulations were being promulgated, archivists and historians testified at Congressional hearings about the impact that the act would have on historical research.\(^{42}\)

2. Overview of HIPAA’s Provisions

HIPAA’s privacy standards are promulgated and administered through the Department of Health and Human Services and its regulations in the Privacy Rule.\(^{43}\) The Privacy Rule applies to health plans, health care clearinghouses, and certain health care providers.\(^{44}\) In many cases, historical health sciences special collections are a unit of a college or university that has a medical school or other health sciences departments. In other cases, the historical health sciences special collections are a unit of a hospital or other health care institution. These are institutions to which HIPAA will usually apply, either to the entire organization or to part of it.\(^{45}\) Within that context, the first point of decision for a special collections custodian is to determine whether the collection is considered to be part of a covered, non-covered, or a hybrid entity.\(^{46}\) The Privacy Rule applies only to covered entities and to the covered portions of hybrid entities.\(^{47}\) In many cases, the parent organization will have already made this determination, and the

---

38. HIPAA, supra note 30; see also Lawrence, supra note 35, at 426.
39. Lawrence, supra note 35, at 426.
42. See id.
44. 45 C.F.R. § 160.102-103 (2011).
45. Lawrence, supra note 35, at 431-32.
46. Wiener, supra note 32, at 17.
47. 45 C.F.R. § 164.103, 160.102, 160.103 (2011); SUMMARY OF HIPAA, supra note 43, at 15.
special collections custodian may look to a privacy officer for help in
determining this status and whether, in the case of a hybrid entity, the special
collections are covered or not.48

Once an organization has been designated as a covered or a hybrid entity, the
Privacy Rule applies to “protected health information” (PHI), a subset of
individually identifiable health information that includes specific address
identifiers like, telephone, numbers, email addresses, and other similar
identifiers, various sorts of health record numbers, Social Security numbers,
license numbers, vehicle identifiers, biometric identifiers, and identifiable
photographic images.49 PHI must be redacted before information can be freely
shared.50 Because the Privacy Rule applies to information held by covered
entities on April 14, 2003, it covers information in many documents that were
created many years prior to that date, even if the subjects are deceased.51 For
example, the provisions of the Privacy Rule would govern the use of PHI in
nineteenth-century records if held by a hospital that is a covered entity today.52

The Privacy Rule has many provisions for situations where an entity may
disclose PHI, and one of these is disclosure for research purposes.53 In most
cases, the entity must confine the disclosure to the minimum amount necessary.54
Beyond that, the Privacy Rule imposes a number of additional conditions on
disclosure of PHI for research purposes.55 One situation where the Privacy Rule
allows disclosure is when the subjects have given an authorization.56 Such an
authorization must be specific to the research at hand, not for future, undefined
research projects.57 Without authorizations from the subjects, an entity may
disclose PHI under the following conditions: (1) when an institutional review
board (IRB) or privacy board has issued a waiver; (2) when the researcher, in
certain situations, can show that the PHI will be used for a research protocol only
or for some similar purpose; or (3) when the PHI is only from decedents.58 In the
last instance, the researcher must be able to document the death of the subjects if
necessary.59

49. 45 C.F.R. § 164.514(e)(2) (2011); see also Wiener, supra note 32, at 17.
51. 45 C.F.R. § 164.502(f) (2011); see Wiener, supra note 32, at 17-18; see also Lawrence,
supra note 35, at 436.
52. See Wiener, supra note 32, at 17-18.
53. U.S. Dep’t Health Hum. Servs., Protecting Personal Health Information in
Research: Understanding the HIPAA Privacy Rule 11-13 (2003),
Protecting Personal Health Information].
54. See generally id.
57. Protecting Personal Health Information, supra note 53, at 11-12.
58. Protecting Personal Health Information, supra note 53, at 13-17.
59. Protecting Personal Health Information, supra note 53, at 17.
As an alternative, a researcher may use a limited data set with PHI redacted without restrictions.60 The covered entity that supplies the data must have “no actual knowledge that the remaining information could be used alone or in combination with other information to identify the individual who is the subject of the information.”61

3. HIPAA’s Conflict with the Purposes of the Historical Researcher and Historical Collections Custodian

From its inception, custodians of historical special collections and archives have seen the HIPAA Privacy Rule as problematic because of its lack of a “grandfather” date and because of its rules around use of health information are geared toward the needs of scientific, not historical researchers.62 Despite the testimony of prominent archivists and special collections curators at the time it was adopted, the Privacy Rule reaches forever into the past.63 The rationale for this long reach was a concern that health information about genetic problems and inherited conditions from the past would be used to discriminate in the present.64 Because IRBs were already overburdened with dealing with approving research with human subjects under the Common Rule, many institutions set up privacy boards to deal with HIPAA authorizations and waivers.65 In many cases, there have been reports that, from the historians’ point of view, researchers were incorrectly denied waivers or were given inaccurate information.66

Increasingly, there is a belief that HIPAA will become the “floor” for correct handling of privacy and confidentiality issues in historical health sciences research, even if its requirements are not tailored to this kind of research.67 This trend is seen in a recent proposal to strengthen privacy and confidentiality requirements under the Common Rule for research with human subjects even when HIPAA does not apply.68

60. Protecting Personal Health Information, supra note 53, at 15-16.
61. Protecting Personal Health Information, supra note 53, at 10. But see Paul M. Schwartz & Daniel J. Solove, The PII Problem: Privacy and a New Concept of Personally Identifiable Information, 86 N.Y.U. L. Rev. 1814, 1845-47 (2011) (discussing the ease of identifying individuals even after many pieces of personally identifiable information are redacted). See also Mages, supra note 6, at 129-148 (example of analyzing HIPAA requirements for a primary research document from the 1880’s).
62. See McCall, supra note 421, and Novak, supra note 41.
63. See Novak, supra note 421. (At the time of the publication of this article there have been discussions about modifying HIPAA’s reach into the past, but they are not law. Modification to the HIPAA Privacy, Security and Enforcement 75 Fed. Reg. 40868 (proposed July 14, 2010). The Society of American Archivists supports these changes.) Letter from Helen Tibbo, Society of American Archivists President to Dept. of Health and Human Servs. Office for Civil Rights (Sep. 13, 2010) (available at http://www2.archivists.org/sites/all/files/SAA_HIPAA_091310.pdf).
64. Lawrence, supra note 35, at 438.
65. Lawrence, supra note 35, at 451-52.
66. Lawrence, supra note 35, at 423.
Similarly, institutional privacy officers may not start with a clear sense of what special collections contain or when the Privacy Rule may apply. Among many custodians, there is great concern that the legitimacy of the historical record may be affected because of this lack of knowledge, because collections may be fragmented or de-accessioned, or custodians will be forced to stop collecting certain types of materials. Collection custodians must be prepared to educate legal counsel and privacy professionals about the scope and mission of their collections.

Many historical health sciences collections custodians are keenly interested in digitizing their collections in order to facilitate access for researchers that cannot physically travel and to reduce wear and tear on fragile materials. The trend in many special collections projects is mass digitization, where material is converted to digital form as quickly as possible without extensive analysis of the content. This may be impossible or unwise when dealing with historical health science collections because of the need to examine material closely to look for privacy and confidentiality breaches and issues.

B. Other Privacy and Confidentiality Laws

Although HIPAA causes the most concern among custodians of historical health sciences special collections, other privacy and confidentiality laws are also relevant and may have requirements to which custodians must adhere. These include other federal laws, most notably the Federal Educational Rights and Privacy Act (FERPA) in educational settings, and state privacy and confidentiality laws.

FERPA is foremost among federal statutes, other than HIPAA, that may have a bearing on the historical health sciences special collections. These collections often include records from medical schools and nursing schools that are heavily used and consulted. FERPA applies when the Department of Education provides funding to an educational institution. FERPA gives control of records to each student and provides limits on the situations under which an institution can release these records. In addition, many institutions have their own policies with regard to student records, and there may be requirements to

69. Gilliland, supra note 4, at 400.
70. Novak, supra note 42.
71. Gilliland, supra note 4, at 400.
72. Gilliland, supra note 4, at 397.
73. Gilliland, supra note 4, at 387-90.
75. Gilliland, supra note 4, at 387-90.
76. See FERPA, supra note 74.
77. Gilliland, supra note 4, at 387-88.
78. Id. at 387; see also FERPA, supra note 74.
79. Gilliland, supra note 4, at 387-88.
comply with state open records laws and other statutes.\(^{80}\) FERPA has no provision for a private remedy, and penalties and enforcement are handled on an institutional basis through the Family Policy Compliance Office.\(^{81}\) When they apply, FERPA regulations add another layer of compliance and concern for the custodian of historical health sciences collections.\(^{82}\)

State privacy and confidentiality laws may provide a cause of action when HIPAA does not apply (such as when a special collection is not a covered entity), when these laws provide greater protection than HIPAA provides, or when a subject pursues a private remedy.\(^{83}\) Most actions will be subject to relevant statutes of limitations and, in many jurisdictions, require that the breach of privacy or confidentiality involve living people.\(^{84}\)

Traditionally, “the common law tort of breach of confidentiality” and the physician’s code of ethics governed the confidence and privacy of the communications between patient and doctor.\(^{85}\) While there was no common law privilege that governed the admissibility of communications to a physician in court, the privilege was instituted by statute during the 19th century.\(^{86}\) Outside the realm of the courtroom, if a patient felt that a physician had breached that duty and sought redress through the courts, the action was predicated on the law of confidence, not privacy.\(^{87}\) Under this legal theory, a plaintiff suffers injury when a trusted relationship is damaged by a betrayal of a confidence.\(^{88}\) As Neil M. Richards and Daniel J. Solove point out, “the focus of the tort of breach of confidentiality is on the nature of the relationship” and the “norms of trust within relationships.”\(^{89}\)

Although the law of confidence continued to develop robustly in the United Kingdom, in the United States the notion of privacy supplanted it to a large extent when Brandeis and Warren published their famous article, “The Right to Privacy,” in 1890.\(^{90}\) One of their arguments was that the technological innovations\(^{91}\) of the day made it necessary for the law to protect not only confidential relationships between people, but also to protect the disclosure of

\(^{80}\) Gilliland, supra note 4, at 388.
\(^{82}\) Gilliland, supra note 4, at 388.
\(^{83}\) Gilliland, supra note 4, at 390-91.
\(^{84}\) See generally DANIEL J. SOLOVE & PAUL M. SCHWARTZ, PRIVACY LAW FUNDAMENTALS (2011) [hereinafter PRIVACY LAW FUNDAMENTALS]; and Gilliland, supra note 4, at 390-91.
\(^{85}\) Peter A. Winn, Confidentiality in Cyberspace: The HIPAA Privacy Rules and the Common Law, 33 RUTGERS L.J. 617, 622 n. 11 (2002).
\(^{87}\) Id. at 134-138, 156-58.
\(^{88}\) Id. at 126.
\(^{89}\) Id. at 174.
\(^{90}\) Samuel D. Warren & Louis D. Brandeis, The Right to Privacy, 4 HARV. L. REV. 193 (1890); see also Richards, supra note 86.
\(^{91}\) Richards, supra note 86, at 128.
information outside of these relationships. Newspapers were growing and proliferating rapidly, spreading celebrity gossip and human-interest stories. Eastman Kodak had recently invented a small camera that could take un-posed snapshots without the subjects’ knowledge or consent. Consequently, Warren and Brandeis argued that “the doctrines of contract and of trust [were] inadequate to support the required protection.” A right of privacy was needed to protect people “against the world.”

In Roberson v. Rochester Folding Box Co. in 1902, a New York court held that a woman could not recover damages for an invasion of privacy, and, as a result, that state provided for a right of privacy by statute. Other states followed suit and also began to recognize the right of privacy through the courts or by statute, using some version of the reasoning that Warren and Brandeis had advanced. By 1960, privacy law had developed to the point where William Prosser defined four privacy torts: (1) public exposure of private facts of an embarrassing nature; (2) placing one in “false light in the public eye;” (3) appropriation of plaintiff’s “name and likeness” for the defendant’s advantage; and (4) intrusion into the plaintiff’s “seclusion or solitude.”

Within the context of health care, the public disclosure of private facts is the privacy tort most likely to provide a cause of action if medical confidences or embarrassing information comes to light. This tort is defined as a public disclosure, usually through wide dissemination, of private information that is “highly offensive to a reasonable person” and not of legitimate public concern. Within a special collection of historical medical information, subjects of records might have a cause of action if embarrassing information, such as information about venereal disease, illegitimacy, or mental disorders, is disseminated as a result of digitizing collections. In addition, digitization and dissemination of personal information that is not highly offensive, such as Social Security numbers, also may cause harm to subjects.

The tort of false light occurs when private facts are exposed in a way that leads to true but highly inaccurate impressions, such as the stories peddled by sensational tabloids. It is unlikely that this tort would form the basis of a
cause of action for the subject of historical medical special collections material, particularly because the entity disclosing the information must have acted with “actual malice or a reckless disregard for the truth.”$^{105}$ However, occasionally the subjects of digitized historical information have sued on the basis of defamation, false light’s close cousin.$^{106}$ At first blush, it appears unlikely that the tort of misappropriation of a name or likeness could form a cause of action in the context of historical health sciences special collections. However, some archives choose to sell images from their collections for the purpose of generating profit, and so this might be a cause for concern where this is a source of revenue for an institution.$^{107}$

In contrast, the law of confidence has developed more slowly in the United States.$^{108}$ Nevertheless, most states recognize the tort of breach of confidence between physician and patient, with many also recognizing tort liability for a third party who induces such a breach.$^{109}$ There is a sense that the law of confidence may form the basis of a cause of action in more situations in the future. Unlike the privacy torts, there is no requirement that information exposed be offensive and there are fewer issues of free speech and public concern.$^{110}$ In the context of historical health sciences special collections, a breach of confidence is most likely to be a concern when the subject or subjects are still living, when information is relatively recent, and where the donor or original owner of the information had a “duty of confidence toward the subjects.”$^{111}$

C. Changing Expectations of Privacy and Confidentiality

As previously discussed, medical records have historically contained sensitive patient information and patients expected that their physicians would safeguard medical privacy and confidences.$^{112}$ Patients generally trusted that their medical information would be kept private and physicians were entrusted to uphold this expectation. As some records moved from files in current use to those deemed historically significant, archivists held to the same privacy protection expectations.$^{113}$ However, record sharing through the advancements

---

$^{105}$ Gilliland, *supra* note 420, at 389.


$^{107}$ Gilliland, *supra* note 4, at 390.


$^{110}$ Privacy Law Fundamentals, *supra* note 84, at 72-73.

$^{111}$ Gilliland, *supra* note 4, at 390.

$^{112}$ See *supra* Part II A.

$^{113}$ Craig, *supra* note 12, at 246-47.
in technology has meant that patient records can be shared with a larger audience and possibilities for widespread privacy breaches have become a reality. Therefore, it was not the nature of the medical or archival profession, patient expectations, or even the records themselves, but the development of technological means of sharing the records that led to much of the legislation that now governs the use and transfer of privacy-sensitive medical information.\footnote{114}

Custodians of historical health sciences special collections must contend with conflicting expectations of privacy from a variety of sources. Some of these conflicts arise from the fact that the collections deal with material that was created and collected at a variety of different times in history, including times when different situations were considered offensive and the role between health care provider and patient was more paternalistic than it is at present. Donor expectations, especially when those donors were physicians or other health care providers, have also changed over time.\footnote{115} Although there is greater sensitivity to health care privacy in general, today many custodians face considerable pressure to digitize collections, often without a chance to perform a complete inventory in order to determine if those collections contain private information.

1. Expectations of More Privacy

Undoubtedly, the expectations of privacy that have had the greatest impact on historical health sciences special collections come from HIPAA.\footnote{116} Even as they were being promulgated, the provisions of HIPAA’s Privacy Rule generated concern among custodians of these collections.\footnote{117} When HIPAA does not apply, such as when PHI has not been generated by covered entities, the Privacy Rule’s requirements have caused custodians to assess health-related privacy and confidentiality issues more stringently. For example, it is not unusual for historical health sciences collections to contain many images.\footnote{118} In the past, the historical health sciences special collections’ parent institutions probably collected photographs of patients and published them widely without permission from their subjects.\footnote{119} Today, such photographs would only be taken with express permission.\footnote{120}

The rise of the Internet is also responsible for these greater expectations of privacy in two ways. First, the average person has a greater awareness of privacy and the ability to lose his or her privacy than in the past because of the intrusions of social media and the ability to broadcast information more broadly

\footnote{114.}{Carpenter, supra note 29.}
\footnote{115.}{See supra Part III.}
\footnote{116.}{See generally Lawrence, supra note 35.}
\footnote{117.}{See generally Novak and McCall, supra note 41. See also Lawrence, supra note 35, at 436.}
\footnote{118.}{Gilliland, supra note 4, at 390.}
\footnote{119.}{Gilliland, supra note 20, at 385.}
\footnote{120.}{Gilliland, supra note 4, at 385.}
through electronic channels. This is seen explicitly in HIPAA’s concern with ongoing issues with regard to genetic disease and insurance coverage and with its emphasis on information transmitted electronically.

Second, the ability to digitize historical records carries with it the possibility of exposing them to wider view. When it is feasible, most custodians will find it desirable to digitize material in order to preserve fragile formats and allow off-site researchers to use material. It is highly likely that extensive archival holdings have not been inventoried at a detailed level. However, if material is placed on the open Internet without assessment, it is possible that it will contain PHI that should not be disseminated widely. It is possible to digitize material and still limit access, but there must be a detailed audit and inventory of what information is present before a custodian can make those decisions.

2. Desire & Expectations for Less Privacy

Ironically, the use of the Internet and electronic communication also leads to a desire for less privacy and, in many situations, a false sense of security online. This is true even in the arena of health information. For example a number of social media sites encourage people with medical conditions to share information about their symptoms and medications online. Sites such as CaringBridge.org and patientslikeme.com encourage the use of access controls or the use of pseudonyms in order to maintain some measure of privacy online. In most cases, the patient himself or herself, or a close family member, posts the information, not a third party or a health care provider. Nevertheless, some sites encourage the posting of extensive information, such as the results of medical tests, medication dosages, side effects, surgeries, and so on.

Often the impulse toward revealing health information online may come from a false sense of anonymity. Someone who reveals health information may believe that a pseudonym is sufficient enough to protect his or her privacy, not realizing how it may be possible to narrow down that person’s identity. A person with a health condition may not realize how data mining, tracing IP addresses, or facial recognition software can be used to identify people even

122. Lawrence, supra note 35, at 436-438
123. Gilliland, supra note 4, at 393.
124. See supra Part III.
125. Gilliland, supra note 4, at 396-97.
129. Id
130. See FUTURE OF REPUTATION, supra note 126, at 146-48.
when names and addresses are redacted or suppressed. The custodian of a historical health sciences collection should be aware of these trends and possibilities in the protection of personal health information.

3. Privacy in Context

One way to think about privacy is to think of it less as a series of absolutes and more as norms that appear within a context and can vary in relationship to that context. Helen Nissenbaum refers to this concept as “contextual integrity,” which she defines as “compatibility with presiding norms of information appropriateness and distribution.” Determining a privacy violation involves analysis of “several variables, including the nature of the situation…the nature of the information…the roles of agents receiving information; their relationships to information subjects; on what terms the information is shared by the subject; and the terms of further dissemination.”

Although this contextual analysis makes for more variable and relativistic judgments about what constitutes a privacy breach, Nissenbaum argues that this approach is a strength that makes privacy analyses more flexible. In her view, there are two reasons this flexibility is needed. The first is because the “norms of privacy in fact vary considerably from place to place, culture to culture, period to period; this theory not only incorporates this reality but systematically pinpoints the sources of variation.” In addition, restrictions on dissemination of information (which Nissenbaum calls “flow”) “will be a messy task, requiring a grasp of concepts and social institutions as well as knowledge of facts of the matter.”

This approach avoids the pitfalls of basing privacy on a set of protected elements, an approach that may fail in certain situations, or when new tools and technologies are introduced. Ironically, it prefigures a return to the common sense rules and the professional best judgment that historical health sciences collections custodians employed before privacy laws were strengthened.

IV. SOLUTIONS AND STRATEGIES

When the absolute strictures of HIPAA do not apply, it makes sense for the custodian of a historical health sciences collection to use the contextual approach in assessing privacy issues with regard to their collections because these

134. Id.
135. See generally Nissenbaum, supra note 133
137. Nissenbaum, supra note 133, at 156.
138. Nissenbaum, supra note 133, at 156.
collections are excellent examples of the variability in assessing privacy norms “from place to place, culture to culture, period to period.” Material may have been created and collected in a very different milieu from the one in which it exists today. The custodian of historical health sciences collections thinks in terms, not only of contemporary norms and needs, but also on what the collection says about past attitudes and on what materials will be useful to researchers in the future. This sensitivity to context makes the custodian an ideal person to make the assessment of contextual integrity that Nissenbaum posits. Factors in a custodian’s assessment that correspond to Nissenbaum’s list include: the age of the material; the kind of symptoms or situations represented; the subjects’ awareness that the material exists and was collected; the likely audience for the material; the donor and his or her situation; and the probability of wide dissemination of the information. The institutional position on privacy and confidentiality matters and the institutional appetite for risk is also a part of that calculation.

It is essential that custodians of historical health sciences special collections be aware of the institutional climate in which they work and communicate with legal counsel about privacy and confidentiality concerns. Because of the Privacy Rule’s breadth and complexity, it has not been well understood within the community of historians, archivists, and historical health sciences collections custodians. Conversely, it is unlikely that the average institutional privacy officer or institutional in-house legal counsel is aware of the needs and norms of historical research. In many situations, these individuals may not be aware that historical health sciences exist, have a good idea of what they include, or completely understand their importance.

A. HIPAA Compliance for Historical Health Sciences Special Collections

The first question to answer in determining HIPAA compliance for historical health sciences special collections is whether the institution to which the collection belongs is a covered, non-covered, or hybrid entity. If the institution is a hybrid entity, the next assessment is whether the collection is part of the covered or non-covered portion. If the collection is considered part of a covered entity, either because the entire institution is covered by HIPAA or because the collection is in the covered part of a hybrid institution, then the
custodian must abide by the Privacy Rule in handling the material.\footnote{149} Collections must be presented with PHI redactions unless researchers have proper authorization from subjects, subjects are deceased and the research is necessary, or the researcher has obtained a waiver from an Institutional Review Board or Privacy Board.\footnote{150}

Custodians of historical health sciences collections must be prepared to explain the HIPAA regulations to historical researchers who may not be familiar with these legal matters within the health sciences. At the same time, members of Institutional Review Boards, which normally handle ethical treatment of human subjects under the Common Rule, may not have a good understanding of the norms and necessity of historical research.\footnote{151} Consequently, custodians of historical health sciences collections may prefer to institute special Privacy Boards to deal with HIPAA waivers for historical research.\footnote{152}

B. Compliance with other Privacy and Confidentiality Laws

If the institution is not covered, HIPAA does not apply, but resources may still contain personal health information or other privacy-sensitive material. In this situation, a custodian will still need to assess material and consult with institutional legal counsel or other appropriate authorities in order to make an assessment on whether and when to restrict access.\footnote{153}

Liability is one question of interest in analyzing privacy and confidentiality breaches in conjunction with historical health sciences collections. If a donor has violated a confidential relationship or the privacy of subjects, technically the donor should be the first at fault.\footnote{154} Ideally, donor restrictions and agreements at the time that gifts are made will be predicated on the risk of such a breach, but this is not always the case.\footnote{155} In other cases, the provenance of material may be obscure or unknown. Some have posited that the custodian of the collection must have knowledge of the confidential or private material or have acted willfully, and that this may cut off liability.\footnote{156}

There is little case law in this area, which probably indicates that most disputes are handled through donor agreements, careful vetting at the time collections are acquired, or by private settlements when controversies arise.\footnote{157} One of the few cases that dealt with some of these issues involved the Brown...
and Williamson Tobacco Papers and the Tobacco Archives at the University of
California, San Francisco (UCSF).  

The controversy began in 1994 when Stanton Glantz, an anti-smoking
activist and professor at UCSF, received a large number of papers from an
anonymous donor calling himself “Mr. Butts.” The papers were copies of
documents from Brown and Williamson’s research, policy, and marketing that
included increasing evidence that the company knew that nicotine was
addictive. Some documents were from medical and health-related studies. “Mr. Butts” also sent copies of the documents to the New York Times and
Congressman Henry Waxman.  

“Mr. Butts” was actually a paralegal named Merrell Williams who had
worked for one of Brown and Williamson’s law firms. A former smoker with
health problems, Williams had become increasingly troubled by the contents of
the documents he was handling and convinced that Brown and Williamson was
sending incriminating documents to its attorney to protect them as attorney work
products and by attorney-client privilege. He embarked on a concentrated
campaign to find and copy problematic documents during the course of his
work. Both Brown and Williamson and Williams alleged fraud—Brown and
Williamson because Williams violated a confidentiality agreement when he
copied the documents and Williams because the tobacco company had falsely
claimed that the documents were privileged.  

Glantz gave the papers to the UCSF library and archives. As word spread
that the documents were available at UCSF, traffic became unmanageable for the
librarians, so they digitized the documents, first as a CD-ROM, the medium of
choice at that time, and then on the Internet. Initially, the librarians were
concerned about the uncertain provenance of the papers and the precedent they
were setting in accepting the documents and making them available. Were the
documents legitimate? Those concerns came to an end in the winter of 1995,
when Brown and Williamson realized that UCSF had copies of the documents and requested for the library to turn them over.\textsuperscript{169} When UCSF refused, the tobacco company sued.\textsuperscript{170} Brown and Williamson lost at trial and on appeal, despite Merrell Williams’s violation of his confidentiality agreement, in part because UCSF had made the documents available to researchers and started digitization plans.\textsuperscript{171} To cut off access to the documents after those actions would have been a constitutionally unacceptable prior restraint on free speech. In addition, as the judge pointed out, other copies of the documents existed, and parts had been published or publicized by others as well.\textsuperscript{172} Furthermore, UCSF had not been involved in any wrongdoing: “If the University had in fact been a wrongdoer in obtaining the information, then we would have a very different situation.”\textsuperscript{173}

Although the outcome of this one case does not necessarily predict the course of any other litigation, it is an encouraging precedent for custodians of historical health sciences collections.\textsuperscript{174} Today, all of the documents Glantz received are kept online by UCSF, with a fully developed procedure for handling privileged and confidential documents.\textsuperscript{175}

\section*{C. Digitization and Access Control}

Digitization provides many benefits for historical health sciences collections because of the ability to preserve fragile materials and to provide access to remote researchers. However, if material contains large amounts of PHI that must be redacted before material can be posted online, its usefulness can be limited. One option for digitized material is to still control access to authorized personnel and researchers, thus complying with HIPAA or other privacy and confidentiality laws and norms. If material is to be freely available on the Internet, the custodian should select material where few redactions will be necessary.\textsuperscript{176} The same analyses of “contextual integrity” that are used for general access can also be applied to digitization.\textsuperscript{177}

\begin{itemize}
  \item \textsuperscript{169} Calvert, supra note 158, at 403.
  \item \textsuperscript{170} Calvert, supra note 158, at 394, 403; Cigarette Papers, supra note 158, at 12.
  \item \textsuperscript{171} Brown & Williamson Tobacco Corp. v. Regents of Univ. of Cal., No. 967298 (Super. Ct. Cal S.F. County 1995); see generally Calvert, supra note 158; see also Legacy Tobacco Documents Library, available at http://legacy.library.ucsf.edu/about/about_collections.jsp#ucbw (brief discussion of case at University Of California, San Francisco).
  \item \textsuperscript{172} See Brown & Williamson Tobacco Corp. v. Regents of Univ. of Cal., No. 967298, at 59 (Super. Ct. Cal S.F. County 1995).
  \item \textsuperscript{173} Id. at 56.
  \item \textsuperscript{174} Calvert, supra note 158, at 452-53.
  \item \textsuperscript{175} U.C. San Francisco, Library Documents Designated as Privileged or Confidential, LEGACY TOBACCO DOCUMENTS LIBRARY (2007), http://legacy.library.ucsf.edu/help/docdesignation.jsp.
  \item \textsuperscript{176} Gilliland, supra note 4, at 396-98.
  \item \textsuperscript{177} See supra Part III; see generally Nissenbaum, supra note 133.
\end{itemize}
V. CONCLUSION

Historical health sciences collections play an important role in research, both in the field of the history of medicine and also in a variety of other areas in the sciences and social sciences. These collections exist in a variety of institutions, from large academic medical centers to small hospitals. The requirements of HIPAA, along with other concerns over privacy and confidentiality in the digital age, have made the task of providing access to these collections more complex and onerous. Custodians of historical health sciences collections are likely to consult privacy officers and attorneys for assistance in determining the status of materials under HIPAA and other privacy and confidentiality laws in order to make material available to researchers.

It may take considerable time to determine the HIPAA status of a historical health sciences special collections unit and set up procedures to aid researchers. There may be considerable effort expended in analyzing other privacy and confidentiality issues that these collections represent. Nevertheless, the time and effort it takes to make these analyses is well spent. The social and historical value of these materials is immense. Most materials are irreplaceable and have a unique role in documenting and informing us about our social and cultural heritage.
THE PREOPERATIONAL LEGAL REVIEW OF CYBER
CAPABILITIES: ENSURING THE LEGALITY OF CYBER
WEAPONS

P.J. Blount*

I. INTRODUCTION

In 2011, the United States Department of Defense adopted a policy, as part of its cyber strategy, that cyber attacks could be treated as an act of war and could possibly warrant a non cyber response. An unnamed Defense Department official, who served as the source for the Wall Street Journal story reporting the policy change, stated: “If you shut down our power grid, maybe we will put a missile down one of your smokestacks.” This stance opened up a variety of legal questions for the United States, but clarified its position regarding whether cyber attacks could rise to the level of an armed attack, and thus justifying self-defense measures for purposes of international law. Shortly after making this policy decision, the United States Air Force adopted a new instruction that stated that cyber weapons and cyber capabilities would receive a pre-operational legal review. This new policy signified that the United States is willing to play by its own rules and treat its cyber capabilities as potential weapons.

States have a duty to perform a legal review of weapons before they are used in international armed conflict, in order to ensure that the weapons comport with the laws of international armed conflict (LOIAC); this is primarily to determine that the weapons’ use does not result in unnecessary suffering of combatants or indiscriminate attacks that damage civilians and civilian property. This article provides a brief overview of the general problems related to the use of cyber capabilities in armed conflict, and then turns to analyzing the requirements of a pre-operational review of cyber weapons.

* Research Counsel and Instructor of Law, National Center for Remote Sensing, Air, and Space Law, University of Mississippi School of Law.


2. Id.


5. See generally id.
II. CYBER WARFARE

Since its inception, the Internet has been intertwined with the military.\(^6\) Its initial structure was built at the Defense Advanced Research Projects Agency (DARPA).\(^7\) However, these systems have changed from a military communication network to a worldwide infrastructure, which underlies a great deal of human, economic, and diplomatic interactions.\(^8\) Militaries have not only treated cyberspace as a tool, but have also adopted it as a domain in which they operate.\(^9\) Cyberspace has the potential to be the newest battleground.\(^10\)

In this context, the United States Department of Defense adopted a new policy for cyberspace, which touts that a cyber attack could amount to the use of armed force, and that armed force could be used to retaliate against cyber attacks.\(^11\) This is not surprising and to some extent anticipated, because States tend to interpret international law in order to best pursue their goals and ensure their own security.\(^12\) The stance does, however, highlight some of the foundational legal questions that apply to the cyber use in armed conflict.

Cyber, at its heart, challenges many of the traditional underpinnings of law in armed conflict.\(^13\) For instance, while the use of force is generally recognized as an illegal act,\(^14\) it may be used in self-defense to an “armed attack.”\(^15\) Within this rubric, the question of what constitutes “armed” is paramount to the legality of self-defense, which in turn hinges on the question of what constitutes a “weapon.” Parsing out the various ambiguities is not the purpose of this particular paper. However, when militaries begin to operate in new domains, the legal definitions from the law of armed conflict often become difficult to apply.\(^16\) This has already been seen in the 20th century with the addition of air


\(^7\) See id.

\(^8\) See id.


\(^10\) See id.; see also Vida M. Antolin-Jenkins, Defining the Parameters of Cyberwar Operations: Looking for Law in All the Wrong Places?, 51 NAVAL L. REV. 132, 133 (2005).

\(^11\) While the specific language did not make it into the unclassified version of the document, there has been little, if any at all, speculation that this view is not in the classified version. See generally DEP’T OF DEFENSE, DEP’T OF DEFENSE STRATEGY FOR OPERATING IN CYBERSPACE (JULY 2011), available at http://www.defense.gov/news/d20110714cyber.pdf.

\(^12\) In this particular case, the United States is one of the most networked nations in the world. While this leads to a higher quality of life for its citizens, it also means the U.S. could be more vulnerable to cyber attacks due to its reliance on cyber technologies.

\(^13\) Antolin-Jenkins, supra note 10, at 133.

\(^14\) U.N. Charter, art. 2(4).

\(^15\) U.N. Charter, art. 51.

and space to the cadre of military operations. Cyberspace is no exception, but its lack of a “physical” setting creates new and unique questions for the laws of armed conflict.

The United States’ actions, to some extent, serve not to alleviate the ambiguities in the definitions but more to supersede the need for debate. The declaration that cyber attacks can, under U.S. interpretation, rise to the level of an armed attack serves as an explicit warning to nations employing such tactics, whether for aggressive, defensive, or intelligence uses. In a sense, the U.S. has quashed the need for debate over whether cyber actions constitute force, and moved it to address which types constitute force and what constitutes proper use under the law of armed conflict. This also means that the United States military, which is very reliant on cyber capabilities, must attempt to answer these questions in relation to its own capabilities as well. If the U.S. is going to treat certain actions as attacks, then it cannot use similar capabilities without itself being accused of using illegal force. Making the distinction between capabilities that rise to the level of an attack is critical, due to the military and intelligence community’s reliance on cyber capabilities. Review of these capabilities will inform such communities about their own restraints in using these technologies.

III. THE DUTY TO EVALUATE WEAPONS

The best articulation of the duty to evaluate weapons can be found in the Protocol Additional to the Geneva Conventions.\(^\text{17}\) Article 36 states:

> In the study, development, acquisition or adoption of a new weapon, means or method of warfare, a High Contracting Party is under an obligation to determine whether its employment would, in some or all circumstances, be prohibited by this Protocol or by any other rule of international law applicable to the High Contracting Party.\(^\text{18}\)

While the United States is not a party to Additional Protocol I, the U.S. embraced the duty to evaluate, before its articulation in Additional Protocol I, through a Department of Defense Directive in 1974.\(^\text{19}\) While it is unclear whether this duty extends to the realm of customary international law,\(^\text{20}\) the rule is, to some extent, implied by the rules of armed conflict.

\[^{17}\text{Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 1125 U.N.T.S. 3 (June 8, 1977).}\]

\[^{18}\text{Id.}\]

\[^{19}\text{See Remarks of Michael John Matheson, 1978 PROCEEDINGS OF THE ANNUAL MEETING (AMERICAN SOCIETY OF INTERNATIONAL LAW 26, 27 (1978).}\]

\[^{20}\text{The Law of War Documentary Supplement, published by the United States Army in 2008, includes two documents that discuss the customary international law elements of Additional Protocol I. Both of these documents are silent as to Article 36. See Additional Protocol I as an}\]
The Hague Convention states that “[t]he right of belligerents to adopt means of injuring the enemy is not unlimited.” This implies some responsibility for States to ensure that the weapons they use do not violate the law of armed conflict. In fact, the underpinnings of international humanitarian law reinforce this idea as its purpose is to “[set] limits on armed violence in wartime in order to prevent, or at least reduce, suffering.” If States are not permitted to employ weapons that violate these rules, then there must, at the very least, be an implied duty to evaluate the weapons being developed. This review should have a legal component as the law defines the parameters of acceptable weapons.

IV. THE AIR FORCE INSTRUCTION

Air Force Instruction 51-102 was updated in July of 2011 to “[reflect] a change in the Air Force definition of ‘weapon’ and [require] a legal review of cyber capabilities intended for use in cyberspace operations.” Specifically, the Instruction requires that cyber capabilities, like weapons “being developed, bought, built, modified or otherwise being acquired by the Air Force,” be “reviewed for legality under the Law of Armed Conflict, domestic law and international law prior to their possible acquisition for use in a conflict or other military operation.”

The review is a three-step process. It first requires that the weapon or cyber capability be evaluated to determine “[w]hether there is a specific rule of law, whether by treaty obligation of the United States or accepted by the United States as customary international law, prohibiting or restricting the use of the weapon or cyber capability in question.” If no “express prohibition” is found, then the reviewing officer must examine two specific questions. The first is “[w]hether the weapon or cyber capability is calculated to cause superfluous injury, in violation of Article 23(e) of the Annex to Hague Convention IV.” The second question addresses whether the weapon or cyber capability can target

---

24. Id. at 2.
25. Id. at 3.
26. Id.
27. Id.
a “specific military objective” and, if not, is it “of a nature to cause an effect” on military and civilian objectives without distinction.\(^{28}\)

Interestingly, cyber capabilities are not termed as weapons yet they will receive the same legal review. Weapons, for the instruction’s purposes, “are devices designed to kill, injure, disable or temporarily incapacitate people, or destroy, damage or temporarily incapacitate property or materiel.”\(^ {29}\) Cyber capabilities that require review are “any device[s] or software payload[s] intended to disrupt, deny, degrade, negate, impair or destroy adversarial computer systems, data, activities or capabilities.”\(^ {30}\) Conversely, devices and software that are “solely intended to provide access to an adversarial computer system for data exploitation” do not need legal review.\(^ {31}\) This distinction is very important, and meant to protect intelligence-gathering operations. If cyber capabilities for intelligence-gathering were reviewed as weapons, then a State that was the subject of such intelligence-gathering might be able to claim that it was the victim of an armed attack. Intelligence operations themselves are not illegal under international law.\(^ {32}\)

The decision to segregate cyber capabilities from weapons is an interesting one in light of the “armed attack” requirement from Article 51 of the U.N. Charter. It is very likely based on a perceived need to be careful about what to refer to as a weapon. A weapon, in general, implies that an action involving that piece of technology is armed. By referring to these items as cyber capabilities, the Air Force Instruction avoids the implication of “armed,” but accomplishes the need for compliance with the Law of Armed Conflict. This could very easily be seen as an attempt to have one’s cake and eat it too. However, another interpretation might be that determining when a cyber capability rises to the status of a weapon is difficult; therefore, a legal review of capabilities is necessary.\(^ {33}\) Regardless of the interpretation, the legal review is the same for both weapons and cyber capabilities.

V. SPECIFIC CONCERNS FOR CYBER WEAPONS

As stated, cyber weapons create new problems for both \textit{jus ad bellum} and \textit{jus in bello}. This is because new technology does not fit into the traditional theaters of military operation. While cyber operations are meant to have an effect on the domains of land, sea, air, and space, they do not squarely fit traditional

\(^{28}\) \textit{Id.}

\(^{29}\) United States Air Force, \textit{supra} note 4, at 6.

\(^{30}\) \textit{Id.} at 5.

\(^{31}\) \textit{Id.} at 5.


\(^{33}\) For example, a cyber attack that shuts down substantial infrastructure could be termed an armed attack. \textit{See} Gorman and Barnes, \textit{supra} note 1. Whereas an attack that causes a computer network failure might be argued to be less than armed because of its lack of real space affects.
conceptualizations of weapons. As a result, when applying the law of armed conflict to contemporary technologies, legal reviews of such weapons address novel issues. This section investigates these issues, utilizing the three questions that legal reviewers must ask when reviewing cyber weapons.

A. Whether the Cyber Capability is Outlawed Due to a Rule of Law

The first question is whether the capability violates international or domestic law. This question addresses pure legality: has the specific capability been prohibited by law. A pertinent example of the kind of international law that might prohibit the technology is the Convention on Certain Conventional Weapons. This convention outlaws certain weapons via protocols that are negotiated and ratified by parties to that treaty. To date, there are four protocols that restrict the use of specific weapons, such as land mines and blinding laser weapons among others, in international armed conflict. However, there are no specific limitations on the use of cyber capabilities that have been negotiated at the international level.

Domestic law could also outlaw specific weapons from military use; however, at this time, no such provision relating to cyber capabilities exists. Yet, there are laws that restrict the military in domestic situations. For instance, the Posse Comitatus Act limits the military and its assets from being used in law enforcement. Any cyber capability employed would need to be technically capable of being restricted to use outside the country, rather than on domestic networks and systems.

B. Does the Capability Cause Superfluous Injury

Next, the evaluator must ask whether the capability causes superfluous injury, which is prohibited in Article 23(e) of the Annex to Hague IV Convention of 1907. The Hague Conventions of 1899 and 1907 were some of the first formal negotiations on the Laws of International Armed Conflict and the resulting conventions are still important documents for these laws. Article 23(e) states that it is forbidden to “employ arms, projectiles, or material calculated to cause unnecessary suffering.”

This prohibition is geared toward protecting combatants from weapons that cause unnecessary suffering. Unnecessary suffering is defined as “harm greater

---

34. United States Air Force, supra note 4, at 3.
36. See id.
38. United States Air Force, supra note 4, at 3.
39. Annex, supra note 21, art. 23(e).
It follows that a weapon will not be outlawed simply because it causes horrendous or mass harm, but instead, such a determination requires balancing the interests of the military objective, the harm caused, and the constraints in a given situation. Weapons are deemed illegal when they cause injuries that could have been avoided in a given situation. In any scenario, military lawyers will compare options to find one that avoids the most suffering. However, in the Air Force instruction's test, the lawyer must evaluate whether the weapon is de facto calculated to cause unnecessary suffering. Examples of these types of weapons are most readily found among those that have been explicitly banned. For instance, the international community has banned the use of blinding lasers; the reason for this “is that its impact – permanent loss of vision – is a severe life-long incapacitation, which is irreversible.” Such a weapon is illegal because its purpose is to cause incapacitation that will last long past the end of hostilities.

It is unlikely that a cyber capability would fall into this category. For the most part, cyber capabilities are designed to affect bits and bytes in order to cause real world effects. For a cyber capability to toe this particular threshold would push the constraints of the technology that underlies these sorts of capabilities. While science fiction type scenarios could be postulated, it seems that any real life scenario would necessarily involve a legal review of a particular use in the field of a capability. For instance, a cyber capability designed to shut down infrastructures, such as power stations, would not de facto cause unnecessary suffering, but a particular use of it might.

C. Is the Capability Sufficiently Targetable

The final consideration for cyber capabilities is likely the most critical in the review process for these types of technologies. Legal weapons must be capable of discriminating between combatants and civilians, as well as military objectives and civilian property. The purpose of this rule is to minimize civilian casualties and to minimize damage to civilian property. Most weapons can be used either discriminately or indiscriminately. This does not make the weapon itself illegal, but instead makes a particular use of the weapon illegal. If a weapon is used in an indiscriminate manner, that “does not stain the weapons themselves with an indelible mark of illegitimacy.” This prong of the review makes an inquiry into whether there is a legitimate use of the weapon that can properly discriminate between military targets and civilian targets.

41. Dinstein, supra note 32, at 59.
42. See id. at 60.
43. Id. at 73.
44. United States Air Force, supra note 4, at 3.
45. Dinstein, supra note 32, at 55.
The principle of discrimination is embodied in Rule 1 of the International Committee of the Red Cross’ Commentary on Customary International Humanitarian Law: “The parties to the conflict must at all times distinguish between civilians and combatants. Attacks may only be directed against combatants. Attacks must not be directed against civilians.”46 This rule requires military actors to ensure that their actions do not target civilians. This, of course, does not outlaw the inevitable civilian casualties; instead, it outlaws attacks that either directly target civilians or attacks that are not limited in such a way as to minimize civilian damage. The reasoning behind this principle is obvious: wanton killing of civilians in an armed conflict between States is considered to be particularly evil. The International Court of Justice has referred to this as an “intransgressible” principle of the Laws of International Armed Conflict.47

A civilian is any person not a combatant, and civilian objects are objects that are not military objectives.48 Civilians, according to the ICRC Rule 5, “are persons who are not members of the armed forces. The civilian population comprises all persons who are civilians.”49 Moreover, the ICRC Rule 5 implies that civilian objects are those that are not military objectives,50 and Rule 8 states that “military objectives are limited to those objects which by their nature, location, purpose or use make an effective contribution to military action and whose partial or total destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military advantage.”51 While there are many different formulations of the content of these terms (a debate that sits outside the scope of this paper), this basic rubric can be used to investigate the challenges for new cyber capabilities.

Cyber capabilities are those that “disrupt, deny, degrade, negate, impair or destroy adversarial computer systems, data, activities or capabilities.”52 These capabilities occur through computer networks, and as such are designed to directly affect the computer software of the target computers. This does not mean that these attacks do not have real world effects, as the intent is to use computer networks to degrade a belligerent’s ability to engage in hostilities.53

47. Legality of the Threat or Use of Nuclear Weapons, supra note 40, at 257.
49. Id.
50. See id.
52. United States Air Force, supra note 4, at 5.
53. John B. Sheldon, Deciphering Cyberpower: Strategic Purpose in Peace and War, STRATEGIC STUDIES QUARTERLY, Summer 2011, 95 (2011) (“This strategic purpose revolves around the ability in peace and war to manipulate perceptions of the strategic environment to one’s
prime example of such an attack is the Stuxnet virus that shut down Iranian nuclear facilities. This virus attacked very specific computers that ran specific functions in Iran’s nuclear plant. 54 The result was more than just an interference with the Iranian computers; indeed, it caused the real space disablement of the nuclear facilities. Concerns have similarly been expressed about using such technology to shut down infrastructure, such as power stations or dams. Many scholars have taken issue with the doomsday-type forecasting, and claim that these technologies would not be as devastating as is often predicted. 55

Cyber capabilities could have a widespread effect on civilians. If a computer virus were used to shut down infrastructure such as a dam, then the result could be the death of civilians. The threshold question, then, is whether the technology can be used in such a way that properly distinguishes between civilians and combatants. If the technology shuts down critical infrastructure indiscriminately, then the answer would be no. For instance, shutting down a power station near a major city might result in deaths of that city’s civilian population. While this might further war objectives generally, the weapon could be seen as indiscriminately attacking civilians. This could be comparable to shutting down a nuclear reactor that is believed to cover for nuclear weapons development. However, while the reactor might be providing power to civilians, the objective of keeping nuclear weapons out of a combat zone might be such that shutting off that power source is justified, even though causing a reactor meltdown would most likely not be justified. Stuxnet provides an excellent example of a targetable cyber capability. 56 It specifically affected only the Iranian nuclear infrastructure, as opposed to infected nuclear facilities worldwide. 57

Civilian objects are to be preserved as well. Cyber capabilities create unique challenges for the respect given to civilian objects. This is primarily because the most prominent road for the use of cyber capabilities is the Internet, which is essentially a civilian infrastructure despite its military origins. 58 However, as a result of “use” one can argue that the Internet becomes a place for legitimate military action. 59 Of course, it is more often sub-networks and computers at the “ends” of the Internet that are being targeted. The key question, again, is advantage while at the same time degrading the ability of an adversary to comprehend that same environment.”); See also id. at 96 (“Cyberspace requires man-made objects to exist.”).


56. See Ackerman, supra note 54.

57. See id.

58. See Antolin-Jenkins, supra note 10, at 132-33.

59. I acknowledge that this is a circular argument: the Internet is used by militaries, so its use makes it a legitimate space for military action.
whether such attacks can be limited to the intended targets. For instance, a cyber capability that is intended to disrupt military networks, but also disrupts civilian financial networks, has not been properly limited. Again, as Stuxnet illustrates, cyber capabilities are technologically capable of discriminating and targeting discrete systems. It will be up to the reviewer to ensure that a particular capability can be properly limited.

VI. OTHER ISSUES

The concept of cyber conflict is a complicated matter. This paper only seeks to investigate the review process for cyber capabilities. There is, however, a rich body of literature that investigates related issues that arise from the laws of international armed conflict. The attorneys doing this work for the military need a high level of technical competence in addition to their grasp of legal concepts. Understanding of the architecture and nature of networks will be a requisite for anyone engaged in the evaluation of cyber capabilities. This might require the military to engage in capacity building so that it can ensure that it has properly trained lawyers.

VII. CONCLUSION

The Air Force Instruction serves as an excellent reminder of the U.S. military’s ongoing commitment to its international law obligations. The willingness to evaluate these capabilities in light of international humanitarian law shows that the United States takes seriously the commitment to minimizing damage to civilian objects and preventing civilian suffering. It also serves as a reminder of the strategic ground at stake and the U.S.’s posturing in this arena. The cyber-theater is a valuable one, yet operation in it opens up great risks. The race for cyber power will be one that continually challenges national security, and having the proper, legal tools on hand will be the first step in successful military actions.

60. United States Air Force, supra note 4.
PLAYSTATION IN HOTZ WATER: REQUIRING NOTICE FOR CIVIL DISCOVERY PURSUANT TO THE DIGITAL MILLENNIUM COPYRIGHT ACT (DMCA) TO PREVENT JOHN DOE SUBPOENAS FROM BOILING OVER INTO FIRST AMENDMENT VIOLATIONS

Andrea Laden*

ABSTRACT

* Andrea Costa Laden is a 2012 graduate of the Salmon P. Chase College of Law Joint JD/MBA program. She also holds an undergraduate degree in Economics from the University of Florida. She sat for the Kentucky Bar Exam this past July.

Sony Computer Entertainment America v. Hotz, a now-settled Digital Millennium Copyright Act case, raises a problem that is both likely to recur and be poorly addressed by federal law and the Federal Rules of Civil Procedure. During discovery, Sony requested identifying information corresponding to a large number of anonymous internet users that posted comments on various websites associated with George Hotz. Few of these anonymous internet users were named potential defendants by Sony, and there is no indication that the users were ever notified that their identifying information had been subpoenaed by Sony. Many internet users were concerned by the breadth of Sony’s subpoena, as evidenced by magazine articles, blogs, television reports, and coordinated attacks on Sony’s network.

Part II of this article summarizes Sony Computer Entertainment America, LLC v. Hotz. Part III reviews legislation that is relevant to that case, as well as others brought under the Digital Millennium Copyright Act of 1998. Part IV discusses the protection of anonymous speech under the First Amendment. Part V explores the standards applied in order to balance a civil plaintiff’s right to seek expedited discovery and a defendant’s right to anonymous speech under the First Amendment. Finally, Part VI concludes by identifying particular considerations that arise under the various standards applied, and proposing several possible solutions.

I. INTRODUCTION

This article analyzes the legal viability of Sony’s discovery requests during the now-settled federal copyright case, Sony Computer Entertainment America v.
Sony Computer Entertainment America (“Sony”) brought a claim for damages against George “GeoHot” Hotz (“Hotz”) under the Digital Millennium Copyright Act of 1998 (“DMCA”) alleging that Hotz circumvented protection measures that controlled access to Sony’s copyrighted work on his PlayStation 3 videogame console and offered his technique to the public in violation of the Act. The lawsuit against Hotz, who is noted for his iPhone jailbreak methods, spurred significant backlash against Sony from the hacking and computer science community. This backlash included multiple distributed denial of service (“DDoS”) attacks and other security breaches that temporarily crippled...
Sony’s PlayStation network. As a result, governments across the world are seeking out members of Anonymous for criminal prosecution.

Sony’s discovery requests pursuant to the copyright lawsuit sought identifying information about users who accessed, commented, or viewed information relating to the method developed by Hotz from Bluehost, Inc., YouTube, Google, and Twitter. For some plaintiffs serving John Doe Subpoenas, identification of the speaker is an end in itself. Discovery requests for user identifying information, or John Doe Subpoenas, are controversial.  

10. See Nick Bilton & Brian Stelter, Sony Says PlayStation Hacker Got Personal Data, N.Y. TIMES (Apr. 26, 2011), www.nytimes.com/2011/04/27/technology/27playstation.html (“It remains unclear who the hackers were. Anonymous, a well-known hacking group that has been blamed for previously attacking the Sony and PlayStation Web sites, denied any responsibility; the group’s Web site stated, ‘For once we didn’t do it.’”); see also Ben Kuchera and Ars Technica, Twitter User Tricks Sony into Posting ‘Secret’ PS3 Code, WIRED.COM (Feb. 9, 2011, 3:54 PM), www.wired.com/threatlevel/2011/02/sony_code/.  


15. See generally Kevin Wein, Dendrite v. Doe: A New Standard for Protecting Anonymity on Internet Message Boards, 42 JURIMETRICS J. 465, 476 (2002) (“In many, if not, most instances, the identity of the poster is the relief that is actually being sought.”).

16. Nathaniel Gleicher, John Doe Subpoenas: Toward a Consistent Legal Standard, 118 YALE L.J. 320, 325 (2008) (“Because of the unique structure of the Internet, the identities of most supposedly “anonymous” posters, while impenetrable to the casual observer, are tracked and stored by the websites on which they post and by the Internet service providers (ISPs) that provide them with Internet access. John Doe subpoenas allow plaintiffs to discover the identity of anonymous online speakers from their ISP or from websites they visited. Without a successful John Doe subpoena, a target of anonymous online speech has no way to uncover his or her attackers and no legal remedy.”).  

17. See generally Chilling Effects, http://chillingeffects.org (last visited July 31, 2011) (Chilling Effects is an organization of the Electronic Frontier Foundation and numerous law schools that spreads knowledge regarding protections that the First Amendment gives to online
and, in some situations, illegal. After a temporary restraining order was issued pursuant to this litigation, YouTube users uploaded copies of Hotz’s video entitled “Jailbroken PS3 3.55 with Homebrew.” One such upload has been viewed 15,720 times, meaning that each of those 15,720 users fall within the scope of Sony’s subpoena, which speaks to the breadth of Sony’s discovery request. An unknown number of anonymous speakers fall within the scope of Sony’s subpoena due to comments regarding the information posted by Hotz.

The courts that have addressed this issue have applied a variety of standards to determine when an anonymous speaker’s identity should be revealed. The spectrum of standards that could be applied ranges (in ascending order) from a commercial speech standard, to a prima facie showing of facts, to more stringent hurdles, such as the Four-Factor Standard from themart.com

activities. The organization devotes considerable time to analyzing the controversy surrounding the use of John Doe subpoenas.)

18. See generally Vincent Pelletier, Strategic Lawsuits against Public Participation (SLAPPs) (and other abusive lawsuits), UNIFORM L. CONFERENCE OF CANADA (August 2008) (“A SLAPP [Strategic Lawsuit against Public Participation] can be defined as a lawsuit initiated against one or more individuals or groups that speak out or take a position in a public debate on an issue of public interest. The purpose of SLAPPs is to limit the freedom of expression of the defendants and neutralize their actions by resorting to the courts to intimidate them, deplete their resources and reduce their means of action.”). See also Your State's Free Speech Protections, THE PUBLIC PARTICIPATION PROJECT (July 31, 2011), www.anti-slapp.org/your-states-free-speech-protection/ (listing information regarding state Anti-SLAPP laws).


20. See Complaint, infra note 45 (Sony’s request included information from YouTube concerning the viewing of Hotz’s video entitled “Jailbroken PS3 3.55 with Homebrew.


22. Although anonymity on the internet has a variety of forms, the distinction is outside the scope of this article. See generally L. Detweiller, Identity Privacy, and Anonymity on the Internet, § 3.1, http://cyber.eserver.org/identity.txt (last visited Aug. 14, 2011) (“Simply stated, anonymity is the absence of identity, the ultimate in privacy. However, there are several variations on this simple theme. A person may wish to be consistently identified by a certain pseudonym or ’handle' and thereby establish a reputation under it in some area, providing pseudo-anonymity. A person may wish to be completely untraceable for a single one-way message (a sort of ’hit-and-run'). Or, a person may wish to be openly anonymous but carry on a conversation with others (with either known or anonymous identities) via an ’anonymous return address'. A user may wish to appear as a ’regular user' but actually be untraceable. Sometimes a user wishes to hide who he is sending mail to (in addition to the message itself). The anonymous item itself may be directed at individuals or groups. A user may wish to access some service and hide all signs of the association.”).


25. See infra Part IV.A.

26. See infra Part IV.B.

27. See infra Part IV.C.
a showing of prima facie evidence sufficient to withstand a motion for summary judgment coupled with notice to the user.28

In fact, this general issue arises frequently in federal and state trial courts29 but few appellate level decisions exist to streamline the standards applied.30 The limited availability of appellate precedent is largely because “discovery disputes are not generally appealable on an interlocutory basis and mandamus review is very limited.”31 Although the Hotz case involves an alleged violation of United States copyright law, discovery standards developed in the defamation context are informative.32

The ideal uniform procedure would require anonymous speakers to receive notice before their identifying information is released so that they may file a motion to quash33 because it is unlikely that any party to the litigation is similarly situated to the non-party speaker.34 Motions to quash should be considered anonymously and the judiciary should employ a uniform procedure35 to balance the case-by-case needs of the party seeking discovery and the anonymous speaker’s first amendment rights in a predictable manner so that both know the bounds of their rights and make informed decisions.36 In addition to

---

28. See infra Part IV.D.
30. The Court of Appeals for the Ninth Circuit recently recognized the variety of standards used to balance a civil plaintiff’s need for discovery against an internet user’s right to anonymous speech, but declined to adopt a standard for the circuit. Id. at *7.
31. Id. at *4.
32. See, e.g., Jessica L. Chilson, Unmasking John Doe: Setting A Standard for Discovery in Anonymous Internet Defamation Cases, 95 Va. L. Rev. 389, 430 (2009) (“A useful comparison is to copyright and trademark law, which has developed in the face of similar conditions of international access.”).
33. Nathaniel Gleicher, John Doe Subpoenas: Toward A Consistent Legal Standard, 118 Yale L. J. 320, 330 (2008) (“Although a motion to quash may well be appropriate, without proper notice, John Doe subpoenas can easily become ex parte proceedings.”).
34. Frequently Asked Questions (and Answers) about John Doe Anonymity, CHILLING EFFECTS, http://chillingeffects.org/johndoe/faq.cgi#QID16 (last visited July 31, 2011) (“Under the normal rules of discovery in civil lawsuits, parties to a suit can simply send a subpoena to anyone they believe has information that could be useful. That information doesn't even have to be relevant to the lawsuit, as long as it could possibly lead to the discovery of relevant information. The only way that a court will evaluate an identity-seeking subpoena is if either the ISP or the target of the subpoena files a motion asking the judge to block the subpoena. Unfortunately, in practice that rarely happens. That is because these subpoenas usually have a short, roughly 7-day deadline, and because many people never even find out that their Internet data has been subpoenaed.”).
35. Gleicher, supra note 34, at 325 (“Although John Doe subpoenas are procedural tools, the standards governing them define the extent of First Amendment rights online. A standard that is too permissive severely weakens the ability of citizens to speak anonymously, limiting freedom of speech online. Too restrictive a standard leaves the increasing litany of targets of online harassment with no defense. Only a consistent nationwide standard for John Doe subpoenas will ensure balanced protection for both anonymous online speakers and the targets of anonymous online speech.”).
36. See Chilson, supra note 32, at 433 (“Plaintiffs and anonymous defendants need consistency in John Doe cases immediately, so that they will know the metes and bounds of their Constitutional protection and can make decisions with full knowledge of where the law will stand.
predictability for individual actors, a uniform test may avoid forum shopping by companies seeking to enforce intellectual property rights and minimize the chilling effect on free speech.

II. SUMMARY OF LITIGATION: SONY COMPUTER ENTERTAINMENT AMERICA V. HOTZ

On January 11, 2011, Sony filed a complaint against Hotz, Hector Martin Cantero (“Cantero”), Sven Peter (“Peter”), and Does 1 through 100 (“Doe Defendants”) in the United States District Court for the Northern District of California. Sony requested injunctive relief and damages pursuant to alleged violations of federal law, such as the circumvention provisions of the DMCA, violations of the Computer Fraud and Abuse Act, 18 U.S.C. § 501, et. seq., and contributory copyright infringement under the Copyright Act. In addition to the federal claims, Sony also alleged a violation of a California statute, and state and federal common law claims for breach of contract, tortious interference with contractual relations, trespass, and common law misappropriation. Sony contended that the defendants (1) circumvented effective technological protection measures that Sony employs to protect against unauthorized access to and copying of Sony’s proprietary PlayStation® 3 computer entertainment system (“PS3 System”), and other Sony copyrighted works, and (2) trafficked in circumvention devices and components thereof that enable unauthorized access to and copying of one or more…copyrighted works.

As such, it is necessary that courts not only address the issue clearly, but that they address it uniformly across the country.

37. Kimberly A. Moore & Francesco Parisi, Rethinking Forum Shopping in Cyberspace, 77 CHI.-KENT L. REV. 1325, 1328 (“Where adjudicatory jurisdictions do overlap, the case will likely be decided in the jurisdiction where it is first filed. By strategically choosing the forum, a plaintiff can maximize the expected return from litigation….In as much as the status of plaintiff is randomly determined, the distributional effects have no ex ante impact on individual incentives. However, if some individuals are statistically more likely to be plaintiffs than defendants, such as property rights holders (copyright owner, patentee, or trademark owner), the opportunity for forum shopping may have biased distributional effects with a potential impact on the ex ante incentives of the parties.”).

38. Chilson, supra note 32, at 471 (“Developing a standard that avoids chilling legitimate speech is clearly desirable. The very rationale for protecting anonymous speech under the First Amendment is that it provides the means to express ideas that are important to free and open discourse. A lack of protection could subject a speaker to persecution or otherwise discourage their comment.”).


41. Id. at ¶ 1.

42. Id. at ¶ 2.
Sony claimed that Hotz built on the circumvention method developed by a group of computer hackers known as FAIL0VERFLOW, accessed a “critical level of the PS3 System,” and publicly distributed his refined method, which allowed PS3 System users to run unauthorized or pirated software via the internet. Sony named defendants Hotz, Cantero, and Peter by name and residence; however, of the one hundred Doe Defendants, Sony mentioned only two in the complaint, and noted its plans to “seek leave to amend [the] Complaint to show the true names and capacities of the Other Doe Defendants when, and if, they become known.” Sony indicated that, “Doe 1 is an individual residing in San Francisco, California...known on the internet by the moniker ‘Bushing,’” and that Doe 2 resides in the Netherlands and “is known on the internet by the moniker ‘Segher.”

With the Complaint, Sony filed a motion requesting, among other items, a temporary restraining order barring Hotz from (a) circumventing the technological protection measures in the PS3 System; (b) distributing or trafficking the Circumvention Devices; (c) accessing the PS3 System; (d) obtaining and transmitting Sony’s proprietary information or code; and (e) impairing the confidentiality of information obtained from the PS3 System until a preliminary injunction could be issued. After a hearing on Sony’s motion, Judge Susan Illston granted Sony’s Ex Parte Motion for a Temporary Restraining Order.

On February 2, 2011, Hotz filed a “Motion to Dismiss for Lack of Personal Jurisdiction.” He argued that, “he does not live in California and does not have continuous, systematic or substantial contact with California which would subject him to personal jurisdiction.” Hotz referred to the Ninth Circuit’s three-part test for determining specific jurisdiction, which requires that:

1. [t]he nonresident defendant must do some act or consummate some transaction with the forum or perform some act by which he
Hotz asserted that his purported acts were not directed at California in part because the makers of the PlayStation console are the separate Japanese parent corporation, Sony, Inc. Additionally, he argued that his activities related to the website he maintains at www.geohot.com, which merely posts information and “does not allow users to interact with the host computer or exchange information,” were passive. Finally, Hotz argued that the last prong of the Ninth Circuit test was not met because he had “no meaningful contact with California,” and “his alleged acts [did] not arise from contact with California.”

In response to the arguments Hotz offered in his Motion to Dismiss, Sony sought to collect facts linking Hotz to California. On February 4, 2011, Sony filed a Notice of Motion and Motion for Expedited Discovery, which included requests for the following information from the defendants and/or third parties:

1. All contacts with California by Hotz and/or any third parties working with him on the unlawful conduct at issue in this lawsuit;
2. All of Hotz’s communications with individuals who have used or downloaded the circumvention devices offered by Hotz;
3. All conferences, forums and meetings attended by Hotz in California;
4. All benefits that Hotz has received in connection with his use and distribution of the circumvention devices;
5. All communications with Doe 1 Defendant (“Bushing”), an individual who likely resides in the Bay Area;
6. Information from the content server host on the accessing and downloading of circumvention devices from Hotz’s website;
7. Information from Google concerning Hotz’s discussion of his circumvention activities with others on his interactive blog;
8. Information from PayPal on Hotz’s PayPal account regarding financial benefits obtained by Hotz as a result of his illegal activity;
9. Information from Twitter concerning Hotz’s communications with others via Twitter regarding his efforts to bypass the TPMs in the PS3 System; and

---

56. Defendant’s Motion to Dismiss for Lack of Personal Jurisdiction at 7, Sony Computer Entm’t Am. v. Hotz, No. 11-167 (N.D. Cal. filed Jan. 11, 2011) (citing Data Disc, Inc. v. Sys. Tech Assocs., 557 F.2d 1280, 1287 (9th Cir. 1977)).
57. Id. at 7-9.
58. Id. at 9.
59. Id. at 17.
60. Letter from Plaintiff Re Third Party Jurisdictional Disc. at 1, Sony Computer Entm’t Am. v. Hotz, No. 11-167 (N.D. Cal. filed Jan. 11, 2011).
10. Information from YouTube concerning the viewing of Hotz’s video entitled “Jailbroken PS3 3.55 with Homebrew.”

Later, on March 1, 2011, Sony filed a letter to Judge Joseph Spero, the Magistrate Judge assigned to the case, regarding third party jurisdictional discovery. In the letter, Sony requested that the Court dismiss an *amicus curae* letter from the Electronic Frontier Foundation (“EFF”) that was submitted on February 14, 2011. The EFF letter argued that (1) Judge Spero should adopt the *2themart.com* standard for reviewing discovery requests for anonymous speaker identifying information, and (2) that the Stored Communications Act absolutely prohibits the portions of Sony’s request covering the content of communications left in comments on the private video. Regarding the discovery dispute, Sony’s letter provided that:

[C]ounsel for the parties met and conferred to resolve their dispute as to the scope of the subpoenas to be served on the third party Internet Service Providers (“ISPs”), including Bluehost, Twitter, Google, YouTube, Softlayer and PayPal. As a result of this meet and confer, the parties narrowed the scope of several of the subpoenas and agreed to provide for protection of confidential information obtained through some of the subpoenas through an Attorney Eyes Only designation. [Sony] also agreed not to pursue, as part of its jurisdictional discovery, several of the third party subpoenas originally included in its Motion for Expedited Discovery…Accordingly, the parties agreed that subject to this Court’s entry of an order, [Sony] may proceed to serve its subpoenas on Bluehost, Twitter, Google, YouTube, and Softlayer for purposes of jurisdictional discovery.

Sony also requested that the Court “issue an order allowing [Sony] to serve the third party subpoenas for targeted jurisdictional discovery as agreed upon by the parties.” Judge Spero granted the request.

---

61. Motion to Expedite at 62, Sony Computer Entm’t Am. v. Hotz, No. 11-167 (N.D. Cal. filed Jan. 11, 2011).
63. *Id.* at 2.
65. *Id.* at 3 (citing 18 U.S.C. § 2702).
67. *Id.* at 6.
III. REVIEW OF RELEVANT LEGISLATION

A. Electronic Communications Privacy Act of 1986

The Electronic Communications Privacy Act of 198669 amended Title III of the Omnibus Crime Control and Safe Streets Act of 1968.70 The Electronic Communication Privacy Act of 1986 ("ECPA") is comprised of three titles, which are commonly referred to as: (1) Title I of the ECPA or the Wiretap Act,71 (2) Title 2 of the ECPA or the Stored Communications Act ("SCA"),72 and (3) Title III of the ECPA or the Pen Register and Trap and Trace Statute.73

The SCA is relevant because it protects the privacy rights of customers and subscribers of computer network service providers in three ways: (1) prohibiting unlawful access to some stored communications;74 (2) regulating the manner in which network service providers voluntarily disclose customer communications and records to the government and third parties;75 and (3) mandating that law enforcement officers must follow certain criminal procedure to properly access stored communications from network providers.76 The SCA applies to two classes of network service providers that are covered by the ECPA. The first class provides an electronic communication service,77 which is “any service which provides to users thereof the ability to send or receive wire or electronic communications.”78 The second class provides a remote computing service,79 which is “the provision to the public of computer storage or processing services by means of an electronic communications system.”80 Although intricacies exist, any entity providing electronic communication services and/or remote computing services is referred to as an internet service provider (ISP)81 herein.

70. In re Askin, 47 F.3d 100, 101 (4th Cir. 1995).
78. Id.
80. Id.
81. Internet Service Providers Law & Legal Definition, USLEGAL.COM http://definitions.uslegal.com/i/internet-service-providers/ (last visited Aug. 15, 2011) ("An Internet Service Provider (ISP) is a company that provides third parties access to the Internet. Many ISP also offer other related services such as Web site design and virtual hosting. An ISP has the equipment and the telecommunication line access required to have a point-of-presence on the Internet for the geographic area served. An ISP acts as an intermediary between its client's computer system and the Internet. ISPs take several forms and offer a wide variety of services. They generally charge their customers for Internet access depending on their usage needs and the level of service provided.").
Where disclosure of customer information is concerned, information requests and subpoenas from governmental and non-governmental entities are protected differently by the SCA. Under Section 2703 of the SCA, there are finite ways a government entity, such as law enforcement, may access customer information stored with a provider without the customer’s consent. If the customer information has been in electronic storage in an electronic communications system for less than 180 days, the government’s only option is to use a properly issued warrant. If the customer information has been in electronic storage in an electronic communications system for longer than 180 days, additional options are available. This provision also allows the government to demand limited customer information using only an administrative subpoena. Under Section 2702, the contents of customer communications are tightly guarded; however, both entities providing electronic communication services and remote computing services may disclose customer information, such as identifying information, to any person other than a governmental agency without exception.

B. The Digital Millennium Copyright Act of 1998 and Corresponding Library of Congress Regulations

The Digital Millennium Copyright Act of 1998 ("DMCA") is divided into the following five titles: (1) Title I, the World Intellectual Property Organization Copyright and Performances and Phonograms Treaties Implementation Act of 1998, (2) Title II, the Online Copyright Infringement Liability Limitation Act, (3) Title III, the Computer Maintenance Competition Assurance Act, (4) Title IV, Miscellaneous Provisions, and (5) Title V, the Vessel Hull Design Protection Act. The DMCA was enacted "to protect from digital piracy the copyright industries that comprise the leading export of the United States."

86. See 18 U.S.C. § 2702(a)-(b).
87. 18 U.S.C. § 2702(c)(6) ("A provider described in subsection (a) may divulge a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by subsection (a)(1) or (a)(2))... to any person other than a governmental entity.").
89. Digital Millennium Copyright Act §§ 101-05.
90. Id. at §§ 201-03.
91. Id. at §§ 301-02.
92. Id. at §§ 401-07.
93. Id. at §§ 501-505.
Additionally, Representative Howard Coble of North Carolina stated that one goal of the DMCA was to provide adequate and balanced copyright protection while extending the fair use doctrine to the digital age. The product of this goal is evident in the savings clause in 17 U.S.C. § 1201, which deals with circumvention of copyright protection systems, that “reserves rights, remedies, limitations, or defenses to copyright infringement, including fair use.”

Title I is central to *Sony Computer Entertainment America v. Hotz*. There are two main parts of Title I. First, through scattered provisions found in 17 U.S.C., Congress “implement[ed] two World Intellectual Property Organization (‘WIPO’) treaties: the WIPO Copyright Treaty and the WIPO Performances and Phonograms Treaty.” Second, Title I of the DMCA makes additions to United States copyright law by restricting circumvention of measures designed to control access to a protected work, such as the protections Sony alleged Hotz circumvented. DMCA outlines a specific procedure for a copyright owner to obtain a subpoena for the purpose of identifying an infringer under section 17 U.S.C. § 512(h), however, the procedure was not employed in *Sony Computer Entertainment America v. Hotz* because Sony’s requests were not limited to the identification of alleged infringers. Although Sony’s cause of action arises out of an alleged violation

have done our best to protect from digital piracy the copyright industries that comprise the leading export of the United States.”)

98. 17 U.S.C. §§ 1201-1205 (2006). See also Exemption to Prohibition Against Circumvention, 75 Fed. Reg. 43,825, 43,826 (codified at 37 C.F.R. § 201.40) (2010) (“Section 1201(a)(1)(A) provides, in part, that no person shall circumvent a technological measure that effectively controls access to a work protected under this title. In order to ensure that the public will have continued ability to engage in noninfringing uses of copyrighted works, such as fair use, subparagraph (B) limits this prohibition. It provides that the prohibition against circumvention shall not apply to persons who are users of a copyrighted work which is in a particular class of works, if such persons are, or are likely to be in the succeeding three-year period, adversely affected by virtue of such prohibition in their ability to make noninfringing uses of that particular class of works under this title as determined in a rulemaking. The proceeding is conducted by the Register of Copyrights, who is to provide notice of the rulemaking, seek comments from the public, consult with the Assistant Secretary for Communications and Information of the Department of Commerce, and recommend final regulations to the Librarian of Congress.”).
101. Subpoenas brought under Section 512(h) may only seek identification of an alleged infringer. See 17 U.S.C. § 512(h) (“A copyright owner or a person authorized to act on the owner’s
of the DMCA, the subpoenas sought by Sony are governed by the general requirements of civil discovery. 102

The Library of Congress has the authority to rule on specific uses of copyrighted works that are non-infringing under the DMCA. 103 Effective July 27, 2010, pursuant to the fourth Library of Congress rulemaking on 17 U.S.C. § 1201, 104 the prohibition against circumvention of technological measures that effectively control access to copyrighted works no longer applies to persons who engage in certain non-infringing uses of six classes of copyrighted works. 105 The first exempt class of works consists of motion pictures and DVDs that are lawfully made and acquired; 106 however, this exception is subject to some limitations on the person engaging in circumvention. 107 The second class of works consists of “[c]omputer programs that enable wireless telephone handsets to execute software applications, where circumvention is accomplished for the sole purpose of enabling interoperability of such applications, when they have been lawfully obtained, with computer programs on the telephone handset.” 108 The third class designated by the Library of Congress is reserved for firmware or software that enables a used cell phone to legally connect to a wireless network. 109 The fourth exemption is made for circumvention of protected video games that are accessible on personal computers when the circumvention is done in good faith for certain security purposes. 110 The fifth class 111 includes

105. Id.
107. 37 C.F.R. § 201.40(b)(1) (“Motion pictures on DVDs that are lawfully made and acquired and that are protected by the Content Scrambling System when circumvention is accomplished solely in order to accomplish the incorporation of short portions of motion pictures into new works for the purpose of criticism or comment, and where the person engaging in circumvention believes and has reasonable grounds for believing that circumvention is necessary to fulfill the purpose of the use in the following instances: (i) Educational uses by college and university professors and by college and university film and media studies students; (ii) Documentary filmmaking; (iii) Noncommercial videos.”).
108. 37 C.F.R. § 201.40(b)(2).
109. 37 C.F.R. § 201.40(b)(3) (“Computer programs, in the form of firmware or software, that enable used wireless telephone handsets to connect to a wireless telecommunications network, when circumvention is initiated by the owner of the copy of the computer program solely in order to connect to a wireless telecommunications network and access to the network is authorized by the operator of the network.”).
110. 37 C.F.R. § 201.40(b)(4) (“Video games accessible on personal computers and protected by technological protection measures that control access to lawfully obtained works, when circumvention is accomplished solely for the purpose of good faith testing for, investigating, or correcting security flaws or vulnerabilities, if: (i) The information derived from the security testing is used primarily to promote the security of the owner or operator of a computer, computer system, or computer network; and (ii) The information derived from the security testing is used or
computer programs protected by certain obsolete and malfunctioning dongles. The sixth and final class of exemptions consists of “literary works distributed in ebook format when all existing ebook editions of the work (including digital text editions made available by authorized entities) contain access controls that prevent the enabling either of the book’s read-aloud function or of screen readers that render the text into a specialized format.”

IV. ANONYMOUS SPEECH AND THE FIRST AMENDMENT

The Supreme Court of the United States has acknowledged that, “the Internet-as ‘the most participatory form of mass speech yet developed’… is entitled to ‘the highest protection from governmental intrusion.” Limits on governmental interference with free speech are imposed on the federal government through the First Amendment and extended to the states through the Fourteenth Amendment. In a separate opinion, the Supreme Court of the United States also held that a court order could constitute government action where the order enforces common law in a manner that infringes on the First Amendment. The tradition of anonymous speech and the use of pseudonyms in the United States is well respected by the Supreme Court of the United States. So long as anonymous interactions are not violating the law, users maintained in a manner that does not facilitate copyright infringement or a violation of applicable law.

111. 37 C.F.R. § 201.40(b)(5) (“Computer programs protected by dongles that prevent access due to malfunction or damage and which are obsolete. A dongle shall be considered obsolete if it is no longer manufactured or if a replacement or repair is no longer reasonably available in the commercial marketplace.”).

112. See generally Definition of Dongle, PC MAGAZINE, http://www.pcmag.com/encyclopedia_term/0,2542,t=dongle&i=41699,00.asp#fbid=9dROxqtzFzR (last visited June 19, 2011) (“Originally slang for a plug-in module to copy protect software (see hardware key), the term is used for any small module that plugs in and sticks out of a socket; for example, USB flash memory drives and other USB devices such as a wireless mouse receiver or cellular air card. If it has a short cable, it may also be called a dongle.”).

113. 37 C.F.R. § 201.40(b)(6).


115. See Gitlow v. New York, 268 U.S. 652, 666 (1925) (“For present purposes we may and do assume that freedom of speech and of the press-which are protected by the First Amendment from abridgment by Congress-are among the fundamental personal rights and ‘liberties' protected by the due process clause of the Fourteenth Amendment from impairment by the States.”).

116. N.Y. Times v. Sullivan, 376 U.S. 254, 265 (1964) (“Although this is a civil lawsuit between private parties, the Alabama courts have applied a state rule of law which petitioners claim to impose invalid restrictions on their constitutional freedoms of speech and press. It matters not that that law has been applied in a civil action and that it is common law only, though supplemented by statute.”).

should be able to participate online without fear of being unveiled through litigation.118

A. McIntyre v. Ohio Elections Commission

In 1995, the Supreme Court of the United States held that an Ohio statutory prohibition against distribution of any anonymous campaign literature was an unconstitutional violation of the First Amendment in McIntyre v. Ohio Elections Commission.119 The court asserted that the right to speak anonymously is central to the respected tradition of anonymity in the advocacy of political causes,120 holding that:

Anonymity is a shield from the tyranny of the majority… It thus exemplifies the purpose behind the Bill of Rights and of the First Amendment in particular: to protect unpopular individuals from retaliation—and their ideas from suppression—at the hand of an intolerant society. The right to remain anonymous may be abused when it shields fraudulent conduct. But political speech by its nature will sometimes have unpalatable consequences, and, in general, our society accords greater weight to the value of free speech than to the dangers of its misuse.121

The Court also emphasized that when a law burdens core political speech, the judiciary must apply exacting scrutiny, which will only permit the restriction if it is “narrowly tailored to serve an overriding state interest.”122 Although the subpoena at issue in Hotz was a civil subpoena, the McIntyre decision illustrates the importance of anonymous speech to the United States political system, especially where controversial issues are involved.123 It is well-settled that “an author’s decision to remain anonymous, like other decisions concerning permit for door-to-door advocacy unconstitutional as it applies to anonymous political speech); and Buckley v. Am. Constitutional Law Found., 525 U.S. 182, 200 (1999) (holding a state statute requiring petitioners to wear identification badges unconstitutional).

118. Columbia Ins. Co. v. Seescandy.com, 185 F.R.D. 573, 578 (N.D. Cal.1999) (“People are permitted to interact pseudonymously and anonymously with each other so long as those acts are not in violation of the law. This ability to speak one's mind without the burden of the other party knowing all the facts about one's identity can foster open communication and robust debate. Furthermore, it permits persons to obtain information relevant to a sensitive or intimate condition without fear of embarrassment. People who have committed no wrong should be able to participate online without fear that someone who wishes to harass or embarrass them can file a frivolous lawsuit and thereby gain the power of the court's order to discover their identity.”).

120. Id. at 342-43.
121. Id. at 357 (internal citations omitted) (citing J. S. Mill, On Liberty, in On Liberty and Considerations on Representative Government 1, 3-4 (R. McCallum ed.1947)).
122. McIntyre, 514 U.S. at 347.
123. Id. at 346 (“The First Amendment affords the broadest protection to such political expression in order to assure the unfettered interchange of ideas for the bringing about of political and social changes desired by the people.”) (internal quotation marks omitted) (quoting Roth v. United States, 354 U.S. 476, 484 (1957)).
omissions or additions to the content of a publication, is an aspect of the freedom of speech protected by the First Amendment." 124

B. NAACP v. Alabama ex rel. Patterson

In 1958, the Supreme Court of the United States held, in NAACP v. Alabama ex rel. Patterson, that an order requiring the National Association for the Advancement of Colored People ("NAACP") to produce records including the names and addresses of all members and agents was a denial of due process because it would place a substantial restraint upon NAACP members’ exercise of their right to freedom of association. 125 Patterson stands for the premise that the right to join a membership organization to express one’s views includes a right to anonymity for ordinary rank-and-file members. 126 The Court balanced Alabama’s interest in controlling member fraud or misuse of funds against the chilling effect of membership disclosure on the NAACP’s ability to operate. 127 The Court also indicated that “[i]t is beyond debate that freedom to engage in association for the advancement of beliefs and ideas is an inseparable aspect of the ‘liberty’ assured by the Due Process Clause of the Fourteenth Amendment, which embraces freedom of speech.” 128 When discussing the indispensable liberties of freedom of speech, press, and association, the Court emphasized its decisions “recognize that abridgement of such rights, even though unintended, may inevitably follow from varied forms of governmental action.” 129 Accordingly, it held that it does not matter if the judicial branch solely committed the governmental action, for whether legislative or judicial, an application of state power may be scrutinized for constitutionality. 130 Although it is generally permissible for states to have ordinary information filing requirements about ownership or membership of an association, in the particular situation where this requirement would have a chilling effect on an association’s ability to retain its members, there must be an exception. 131

C. Reno v. ACLU

In a unanimous decision, 132 the Supreme Court of the United States held in Reno that, despite the importance of the congressional goal of protecting children from harmful materials, two statutory provisions enacted to protect minors from indecent and patently offensive communications on the internet

126. Id. at 463-64.
127. Id. at 464-65.
128. Id. at 460 (citations omitted).
129. Id. at 461.
130. Id. at 463.
131. Patterson, 357 U.S. at 464-65.
were unconstitutional intrusions on the freedom of speech protected by the First Amendment.\textsuperscript{133} The Court described the internet as follows:

Anyone with access to the Internet may take advantage of a wide variety of communication and information retrieval methods. These methods are constantly evolving and difficult to categorize precisely. But, as presently constituted, those most relevant to this case are electronic mail (e-mail), automatic mailing list services (“mail exploders,” sometimes referred to as “listservs”), “newsgroups,” “chat rooms,” and the “World Wide Web.” All of these methods can be used to transmit text; most can transmit sound, pictures, and moving video images. Taken together, these tools constitute a unique medium - known to its users as “cyberspace”-located in no particular geographical location but available to anyone, anywhere in the world, with access to the Internet.\textsuperscript{134}

Additionally, the Court echoed the district court’s observation that “at any given time ‘tens of thousands of users are engaging in conversations on a huge range of subjects’…and it is ‘no exaggeration to conclude that the content on the Internet is as diverse as human thought.’”\textsuperscript{135} Distinguishing the internet from heavily regulated media like radio and television broadcasts, the Court decided that unlike other media, (1) the internet has no history of government supervision and regulation,\textsuperscript{136} and (2) internet communications “do not ‘invade’ an individual’s home or appear on one’s computer screen unbidden.”\textsuperscript{137}

The Court recognized that First Amendment protections apply to internet speech because the internet is a “vast democratic forum”\textsuperscript{138} that “provides relatively unlimited, low-cost capacity for communication of all kinds.”\textsuperscript{139} Under Reno, internet speech is protected by the First Amendment with the same vehemence as traditional speech.\textsuperscript{140}

V. STANDARDS APPLIED WHEN BALANCING A CIVIL PLAINTIFF’S NEED FOR EXPEDITED DISCOVERY AND AN INTERNET USER’S RIGHT TO ANONYMOUS SPEECH

A. Motion to Quash under Federal Rule of Civil Procedure 45

The Federal Rules of Civil Procedure establish parameters by which litigants may plead civil lawsuits before federal district courts. Some commentators

\textsuperscript{133} Id. at 849 (Stevens, J.).
\textsuperscript{134} Id. at 851.
\textsuperscript{135} Id. (quoting ACLU v. Reno, 929 F. Supp. 824, 835, 842 (E.D. Pa. 1996)) (internal quotation marks omitted).
\textsuperscript{136} Reno, 521 U.S. at 867.
\textsuperscript{137} Id. at 869.
\textsuperscript{138} Id. at 868.
\textsuperscript{139} Id. at 870.
\textsuperscript{140} Id. at 863.
attribute the mixed bag of civil discovery standards for anonymous internet speech currently used in the courts to a lagging development of procedural rules.\textsuperscript{141} Rule 45 covers subpoenas such as the one at issue in \textit{Hotz}.\textsuperscript{142} Rule 45(c) deals with protecting a person subject to a subpoena,\textsuperscript{143} and on timely motion, requires the issuing court to quash or modify a subpoena\textsuperscript{144} that:

- fails to allow a reasonable time to comply;
- (ii) requires a person who is neither a party nor a party’s officer to travel more than 100 miles from where that person resides, is employed, or regularly transacts business in person — except that, subject to Rule 45(c)(3)(B)(iii), the person may be commanded to attend a trial by traveling from any such place within the state where the trial is held;
- (iii) requires disclosure of privileged or other protected matter, if no exception or waiver applies;
- or (iv) subjects a person to undue burden.\textsuperscript{145}

Arguably, even if protection is not absolute in the face of the DMCA, to the extent that anonymity is protected by the First Amendment, a court should consider whether a subpoena seeking identifying information should be quashed or modified to guard the protected matter of the anonymous speaker - his or her identity.\textsuperscript{146} The Federal Rules of Civil Procedure also dictate how a party must assert that a subpoena requires disclosure of protected matter in Rule 45(d), which deals with duties in responding to a subpoena.\textsuperscript{147} Rule 45(d) also governs the production of electronically stored information,\textsuperscript{148} such as the rule that states a responding party need not produce the same electronically stored information in more than one form.\textsuperscript{149}

\textbf{B. The No New Standard for Anonymous Commercial Speech}

The ‘no new standard’ standard applies the general law of commercial speech to John Doe Subpoenas seeking identifying information related to commercial speech. In 1998, the United States Court of Appeals for the Sixth
Circuit considered the case *NLRB v. Midland Daily News*\(^{150}\) and determined that “the anonymous speech at issue was commercial speech, but declined to establish or follow any particular standard, other than the general and long-standing precepts governing commercial speech.”\(^{151}\) The Court of Common Pleas of Philadelphia County has also declined to adopt a new or different standard to accommodate anonymous speech and noted that “the grafting of new tests onto existing rules threatens to compromise the values protected by other constitutional provisions, including due process, equal protection, and the right to a trial by jury.”\(^{152}\)

In *Midland Daily News*, the NLRB, an independent agency of the United States, sought enforcement of a subpoena seeking documents that identified the source of an anonymous advertisement in the newspaper’s classified section.\(^{153}\) The court determined that the anonymous advertisement was commercial speech, which is protected from unwarranted governmental intrusion although the Constitution affords less protection to commercial speech than to other forms of expression.\(^{154}\) The Sixth Circuit held that the Board failed to persuade the court that the exercise of the subpoena power was the least extensive means by which the Board could reasonably expect to proceed, without unnecessarily burdening the newspaper’s constitutional right to free expression.\(^{155}\)

C. The Prima Facie Showing Standard

Some courts require a plaintiff to make a prima facie showing\(^{156}\) of the claim for which plaintiff seeks disclosure of identifying information related to an anonymous speaker.\(^{157}\) The lowest standard used by some jurisdictions is the motion to dismiss standard (or good faith standard),\(^{158}\) which (1) requires a plaintiff to make a good faith evidentiary showing, and (2) requires the court to

\(^{150}\) *NLRB v. Midland Daily News*, 151 F.3d 472 (6th Cir. 1998).


\(^{154}\) *Id.* at 474 (citing *Cent. Hudson Gas v. Pub. Serv. Comm’n*, 447 U.S. 557, 561-64 (1980)).

\(^{155}\) *NLRB*, 151 F.3d at 475.

\(^{156}\) *BLACK’S LAW DICTIONARY* 1209 (7th ed. 1999) (“Sufficient to establish a fact or raise a presumption unless disproved or rebutted.”).


assess and compare the magnitude of harms that would be caused to the competing interests.159

D. The Four-Factor Standard from 2themart.com

Like the prima facie showing standard, the four-factor standard established by Doe v. 2themart.com seeks to balance competing interests between the anonymous speakers’ First Amendment rights and the rights of the plaintiffs.160 On a motion to quash, the 2themart.com court ruled that the corporate defendant to a shareholder derivative suit was not entitled to the information sought in a subpoena issued to an internet service provider. The subpoena sought the identification of anonymous speakers that posted messages critical of the corporation.161 An important consideration for the court was that “constitutional rights of Internet users, including the First Amendment right to speak anonymously, must be carefully safeguarded.”162 For that reason, the court opined that a high threshold should be enforced for subpoena requests that encroach on that right, and thus, adopted the four-part clear and convincing standard when it held that:

in order to enforce a civil subpoena seeking the identifying information of a non-party individual who has communicated anonymously over the Internet, the party seeking the information must demonstrate, by a clear showing on the record, that four requirements are met: (1) the subpoena seeking the information was issued in good faith and not for any improper purpose, (2) the information sought relates to a core claim or defense, (3) the identifying information is directly and materially relevant to that claim or defense, and (4) information sufficient to establish or to disprove that claim or defense is unavailable from any other source.163

The court found that defendant’s subpoena was issued in good faith, but failed to meet the three remaining requirements.164 The 2themart.com court relied on the principle that identifying information related to anonymous speakers is sufficiently material to compromise First Amendment rights only when the information is needed to advance core claims or defenses.165

161. Id. at 1097.
162. Id. ("The Internet is a truly democratic forum for communication. It allows for the free exchange of ideas at an unprecedented speed and scale. For this reason, the constitutional rights of Internet users, including the First Amendment right to speak anonymously, must be carefully safeguarded.").
163. Id. at 1097.
164. Id. at 1096-97.
165. Id. at 1097; see Silkwood v. Kerr-McGee Corp., 563 F.2d 433, 438 (10th Cir.1977) (in order to overcome the journalistic privilege of maintaining confidential sources, a party seeking to
E. The Summary Judgment Standard

The test established by the Delaware Supreme Court in Doe v. Cahill\(^{166}\) elevates the standard for disclosure of an anonymous speaker to a summary judgment standard.\(^{167}\) Before a plaintiff can obtain the identity of an anonymous defendant through the compulsory discovery process, the plaintiff must support his claim with facts sufficient to defeat a summary judgment motion.\(^{168}\) A plaintiff must further attempt to notify the anonymous poster that he or she is the subject of a subpoena and then, withhold any action to afford the anonymous defendant reasonable opportunity to file and serve opposition to the discovery request.\(^{169}\)

In Cahill, an anonymous internet user under the alias “Proud Citizen” posted two statements regarding a politician’s performance.\(^{170}\) On an interlocutory appeal, the Supreme Court of Delaware decided that the summary judgment standard applies and that the plaintiff is responsible for notifying the anonymous posters.\(^{171}\)

Like the other courts discussed above, the Cahill court was concerned that a low standard would chill internet speech; however, the Cahill court adopted the summary judgment standard because certain plaintiffs, particularly public figures and large corporations, realize unmasking the anonymous speaker is an important form of relief.\(^{172}\) This relief is powerful because:

> The revelation of identity of an anonymous speaker “may subject [that speaker] to ostracism for expressing unpopular ideas, invite retaliation from those who oppose her ideas or from those whom she criticizes, or simply give unwanted exposure to her mental processes.” Plaintiffs can often initially plead sufficient facts to meet the good faith test… even if the defamation claim is not very strong, or worse, if they do not intend to pursue the defamation action to a final decision. After obtaining the identity of an anonymous critic through the compulsory discovery process, a [plaintiff] who either loses on the merits or fails to pursue a lawsuit is still free to engage in extra-judicial self-help remedies; more bluntly, the plaintiff can simply seek revenge or retribution.\(^{173}\)

The high hurdle established by the Summary Judgment Standard may diminish the probability that future plaintiffs will abuse the judicial system to intimidate

---

167. Id. at 460.
168. Id.
169. Id. at 454.
170. Id. at 457 (citing Lyrissa Barnett Lidsky, Silencing John Doe: Defamation & Discourse in Cyberspace, 49 DUKE L.J. 855, 890 (2000)) (internal quotation marks omitted).
anonymous speakers with tactics like Strategic Lawsuits against Public Participation (“SLAPP”)\(^{174}\) in jurisdictions lacking Anti-SLAPP legislation.\(^ {175}\)

VI. PROPOSALS FOR CHANGE

A. Balancing Rights and the Need for Federal Legislation

Some of the standards discussed above are less helpful than others because, depending on the standard adopted, imbalances between the rights of the anonymous speaker defendant and the DMCA plaintiff may emerge. For instance, the No New Standard standard applied in *Midland Daily News*\(^ {176}\) would not be well-applied to the circumstances in *Hotz* because the situations are too dissimilar. *Midland Daily News* was decided outside the internet context in 1998, before the internet was widely available.\(^ {177}\) Additionally, there is no indication in the *Hotz* record that the comments made by anonymous speakers on YouTube, Twitter, and/or Yahoo constituted commercial speech.

The Summary Judgment Standard, although comprehensive, may be too preferential towards anonymous speakers in the DMCA context. The defamation defendant in *Cahill* only posted two relatively innocuous internet postings on a town forum.\(^ {178}\) The reception of defamatory comments may be linked with the reputation of the speaker, thereby minimizing the effect of an anonymous defamatory statement. However, the ramifications of anonymous speech spreading a circumvention measure does not depend on the speaker’s reputation for truthfulness and, depending on the number of followers the speaker has accrued, could cause serious economic damage in an instant. The notice requirement under the summary judgment standard as required in *Cahill* will not achieve the desired results because a DMCA plaintiff is unlikely to have contact information for the anonymous speakers. The ISP is better positioned to give notice to the anonymous speaker.

The summary judgment standard does diminish the probability that plaintiffs will abuse the legal system to intimidate anonymous speakers; however, numerous state legislatures have already developed solutions to that problem. Congress should take note of the various solutions developed by the states and

---

174. See Chilling Effects, supra note 18.
175. See generally Robert D. Richards, A Slapp in the Facebook: Assessing the Impact of Strategic Lawsuits Against Public Participation on Social Networks, Blogs and Consumer Gripe Sites, 21 DEPAUL J. ART TECH. & INTELL. PROP. L. 221, 242-53 (2011) (discussing the importance of Anti-SLAPP legislation to anonymous speech).
176. See supra Part V.B.
178. Cahill, 884 A.2d at 454.
consider drafting its own Anti-SLAPP legislation to address abuse of the legal system without entangling innocent DMCA plaintiffs. Amendments to the Federal Rules of Civil Procedure and/or the SCA should increase the probability that an anonymous user will receive notice of a subpoena demanding identifying information and have an opportunity to respond.

B. Courts Should Adopt the Four-Factor Standard from 2themart.com

The four-factor standard from 2themart.com should be considered by future trial courts approaching this discovery issue. The four-factor standard requires the court to consider the following four factors in determining whether the subpoena should issue: (1) whether the subpoena seeking the information was issued in good faith and not for any improper purpose, (2) whether the information sought relates to a core claim or defense, (3) whether the identifying information is directly and materially relevant to that claim or defense, and (4) whether information sufficient to establish or to disprove that claim or defense is unavailable from any other source. Unlike the summary judgment standard, the four-factor standard is not so high a hurdle as to prevent a plaintiff from acquiring information to build a case because it does not require the plaintiff to show evidence of every element of a claim. Additionally, rather than allowing the courts to weigh different factors for each case, the factors considered are static, which allows both copyright holders and anonymous internet users to act accordingly.

C. Amendment of Federal Rule of Civil Procedure 45

The likelihood that an anonymous user will represent his or her interests by filing a proper motion to quash depends on the anonymous speaker receiving notice of the subpoena. The circumstances in 2themart.com did not require the court to consider whether notice to users should be required. However, the 2themart.com court did acknowledge that:

many civil subpoenas seeking the identifying information of Internet users may be complied with, and the identifying information disclosed, without notice to the Internet users themselves. This is because some Internet service providers do not notify their users when such a civil subpoena is received. The standard set forth in this Order may guide Internet service providers in determining whether to challenge a specific subpoena on behalf of their users. However, this will provide

179. See supra Part V.D.
180. Gleicher, supra note 35.
181. Doe v. 2themart.com, 140 F. Supp. 2d 1088, 1091 (W.D. Wash. 2001) (“InfoSpace notified these users by e-mail that it had received the subpoena, and gave them time to file a motion to quash.”)
little solace to Internet users whose Internet service company does not provide them notice when a subpoena is received.\textsuperscript{182}

Although Rule 45(c)(3)(iii) permits an Internet service provider to file a motion to quash to prevent production of matter protected by the first amendment, such as identifying information of an anonymous speaker, the interests of the Internet service provider and anonymous speaker are not always aligned. Therefore, a requirement that Internet service providers notify affected users when a civil subpoena is received is advisable. Such an amendment to FRCP 45(d) requiring and similar entities to notify any third party user whose identifying information is responsive to the subpoena and allow users time to file a motion to quash before producing the identifying information will protect the interests of anonymous internet users. This issue is unlikely to efficiently progress to appellate courts;\textsuperscript{183} therefore, appellate precedent will not align the varied treatment civil discovery requests for identifying information connected to anonymous speakers receive in trial courts.

The Supreme Court of the United States should revise the Federal Rules of Civil Procedure\textsuperscript{184} to require Internet service providers to notify affected users when a subpoena demanding identifying information of anonymous speakers is received. Notice to anonymous users should be mandatory because it will facilitate the filing of motions to quash by anonymous speakers pursuant to Rule 45. This is an important safeguard because the litigants in an action\textsuperscript{185} and recipients of the John Doe Subpoena\textsuperscript{186} may not represent the interests of the anonymous users. By enabling the anonymous speakers to object to disclosure, the court will receive a more holistic view of the facts upon which to base its decision. An amendment to the Federal Rules of Civil Procedure will guarantee some consistency in the federal courts on this matter and may stimulate discussions in state legislatures regarding changes to state rules. The most

\textsuperscript{182}. Id. at 1095 n.5.

\textsuperscript{183}. See supra Part V.B.

\textsuperscript{184}. 28 U.S.C. § 2072(a) (“The Supreme Court shall have the power to prescribe general rules of practice and procedure and rules of evidence for cases in the United States district courts (including proceedings before magistrate judges thereof) and courts of appeals.”).

\textsuperscript{185}. Litigants are not similarly situated to an anonymous speaker whose information is requested in a John Doe subpoena because one of the litigants requested the information and the other litigant may be motivated to unveil the anonymous speaker’s identity in the event the anonymous speaker will share any portion of alleged liability.

\textsuperscript{186}. Various statutory provisions shield internet companies from liability resulting from statements made by users. See, e.g., Kelly E. Stavnes, Anonymity Protection Versus Subpoena Compliance: What Media Companies Should Consider When Defending User Comments Online, 36 J. Corp. L. 697, 709-10 (2011) (“The Communications Decency Act, in its original form, criminalized the use of telecommunication devices to transmit “indecent” material (unless somehow made unavailable to those under 18) through anti-indecency and anti-obscenity provisions. While some portions of the Act, namely those deemed to inhibit free speech, have been overruled, section 230 continues to absolve those who provide “interactive computer service[s]” of liability for any statements posted by persons other than their own employees.”) (citing 47 U.S.C. § 223; 47 U.S.C. § 230).
logical location for this requirement is in Rule 45(d), which enumerates duties in responding to a subpoena.\textsuperscript{187}

\textbf{D. Amendment of the Stored Communications Act}

The Stored Communications Act ("SCA") should be amended by striking 18 U.S.C. § 2702(c)(6) and incorporating both a provision requiring notice to any user whose identifying information is responsive to a subpoena as well as a time allowance sufficient to allow the user to file a motion to quash before producing the identifying information. Currently, Section 2702 of the SCA neither restricts the sharing of customer information by ISPs in any way\textsuperscript{188} nor requires an entity to give notice to the customer when sharing his or her information.\textsuperscript{189} In fact, Section 2702(c)(6) expressly permits sharing of customer information with "any person other than a governmental entity."\textsuperscript{190} Although the SCA protects the contents of communications from disclosure,\textsuperscript{191} it does not protect the identity of anonymous speakers.

The clause permitting carte blanche sharing of customer information should be stricken. The SCA should be amended to provide a clause permitting ISPs to share customer information only when users are notified and given time to object. Notification is essential to protecting the interests of anonymous speakers because it provides an opportunity to file an anonymous motion to quash the John Doe Subpoena\textsuperscript{192} and brings the breadth of the subpoena to the court’s attention. Due to the nature of discovery, the court may not have the opportunity to apply a standard if no person or entity objects along the way. The anonymous speaker is best-suited to object to overly-broad discovery by filing the motion to quash.

\textbf{VII. CONCLUSION}

Due to the hurried settlement involved in \textit{Hotz}, it is unclear whether the authorized subpoenas were served to Bluehost, Google, YouTube, or Twitter. It is also uncertain whether any identifying information was produced. Although there may be no damage to the anonymous internet speakers in this instance, the \textit{Hotz} case was the subject of significant media attention and discussion in the computer science community.\textsuperscript{193} The order granting Sony’s discovery request

\begin{itemize}
  \item \textsuperscript{187} \textit{Fed. R. Civ. P.} 45(d).
  \item \textsuperscript{188} \textit{See supra} Part II.A.
  \item \textsuperscript{189} \textit{Id}.
  \item \textsuperscript{190} 18 U.S.C. § 2702(c)(6).
  \item \textsuperscript{191} 18 U.S.C. § 2702(a)-(b).
  \item \textsuperscript{192} \textit{See In re Anonymous Online Speakers, supra} note 30.
  \item \textsuperscript{193} \textit{See, e.g., Digital Millennium Copyright Act, supra} note 7 (articles discussing the \textit{Hotz} litigation). \textit{See also Attack of the Show: Sony vs. GeoHot Hacker Lawsuit} (G4tv.com streaming video uploaded Jan. 13, 2011), http://www.g4tv.com/videos/50733/sony-vs-geohot-hacker-lawsuit/ (\textit{Attack of the Show} is also broadcast on television on the G4 television channel).\end{itemize}
may create a chilling effect on internet speech in subjects such as fair use, cyber security, and encryption best practices. Additionally, the lack of enumerated reasoning behind the court’s decision to grant Sony’s discovery requests does not indicate what standard is followed in the Northern District of California, which is home to Silicon Valley, where information technology leaders such as Apple Corporation, Cisco Systems, IBM Corporation, and Google, Inc. maintain offices.\footnote{See Silicon Valley Companies, \emph{The Silicon Valley Gateway}, http://www.siliconvalley-usa.com/companies?f=yes (last visited July 17, 2011); see also Google Offices, \emph{Google}, http://www.google.com/about/corporate/company/address.html (last visited July 17, 2011).}

Due to the lack of appellate activity on this issue, the Supreme Court of the United States should revise the Federal Rules of Civil Procedure to require holders of personally identifying information to notify affected users when a subpoena demanding identifying information of anonymous speakers is received. The most logical location for this requirement is in Rule 45(d), which enumerates duties in responding to a subpoena. This addition to the rules will enable anonymous speakers to make the court aware of their position by filing a motion to quash the subpoena. The amendment to Rule 45 should also outstrip any click-wrap\footnote{See generally David Callan, \emph{How click-wrap contracts benefit over shrink-wrap contracts}, AKÀ MARKETING, http://www.akamarketing.com/click-wrap-shrink-wrap-contracts.html (last visited Sept. 4, 2011) (describing the drawbacks and benefits of both click-wrap and shrink-wrap contracts).} or adhesion agreement between the holder of personally identifying information and the user that lifts all subpoena notification responsibility. A similar amendment to the SCA, which would limit ISP sharing of customer information to situations where the user has been notified and given time to object, is also a possible solution to the notice deficiency currently in place.

Although too cumbersome to be incorporated as an amendment to the Federal Rules of Civil Procedure or the SCA, the 2themart.com standard should be considered by future trial courts approaching this discovery issue. The 2themart.com standard requires the court to consider the following four factors in determining whether the subpoena should issue: (1) whether the subpoena seeking the information was issued in good faith and not for any improper purpose, (2) whether the information sought relates to a core claim or defense, (3) whether the identifying information is directly and materially relevant to that claim or defense, and (4) whether information sufficient to establish or to disprove that claim or defense is unavailable from any other source.\footnote{See supra Part V.D.}
PUBLICITY RIGHTS IN INDIA

Dr. Kalyan C. Kankanala* and Sandeep Hegde M.**

I. INTRODUCTION

Every person has the right to be left alone and lead a private life without any external intervention. This right, referred to as the right of privacy and recognized under common law, has been given the status of a fundamental right under the Indian Constitution. While every person has the right of privacy, the scope of that right dwindles with a person’s increase in popularity and public recognition.\(^1\) Eventually, such increases reach a point where the public may intrude into certain aspects of the life of a popular person or celebrity without liability.\(^2\) In other words, a celebrity’s right of privacy is curtailed by the freedom of speech and expression under the Constitution, which includes the freedom of press and access to information.\(^3\) People can follow certain aspects of a celebrity’s life, and reporting about a celebrity does not amount to violation of his privacy.

Although a celebrity loses the right of privacy to a certain extent, he gains the right of publicity that includes the right to prevent commercial use of his persona.\(^4\) The right of publicity, which springs from public recognition, enables a person to control the commercial exploitation of his persona, including name, likeness, signature, or any other identity.\(^5\) In other words, no person can use any trait of a celebrity to promote commercial products without authorization. Celebrities earn substantial revenues by permitting the use of their persona with

---


\(^{2}\) For example, the President of the United States.

\(^{3}\) See U.S. Const. amend. I (stating that “Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances.”).

\(^{4}\) See Restatement (Second) of Torts § 652(C) (stating that “[o]ne who appropriates to his own use or benefit the name or likeness of another is subject to liability to the other for invasion of his privacy.”).

\(^{5}\) Id.
commercial products, and publicity rights play an important role in preventing false endorsement and the tort of passing off.

By virtue of their popularity, celebrities also play a very important role in influencing society and culture. The general public follows celebrities’ lives very keenly and their behaviour and actions influence social behaviour in many ways. Historically, famous personalities have transformed various aspects of life, ranging from culture to fashion. Considering the personal rights of celebrities and the role that a celebrity can play in the society, it is important that a celebrity’s rights are clearly defined. Certainty with respect to publicity rights is necessary to ensure protection of a celebrity’s endorsement interests, prevent consumer deception, and avoid unjust enrichment.

However, the right of publicity is of recent advent in India and its contours are far from clear. The evolution of modern technology and accompanying legal ambiguity add further uncertainty to the scope and extent of the right. This article elaborates on the ambiguities with respect to the right of publicity in India and elucidates the issues relating to its applicability for computer games. After explaining the issues with respect to the law, the article proposes a publicity right model based on experience in the United States of America and the United Kingdom.

The first part of the article gives a brief account of the right of privacy in India and its evolution as a common law and constitutional right. The second part of the article elaborates on the contours of the right of publicity with the help of case law. The third part analyzes the application of publicity law in India to computer games with the help of a hypothetical case, and the last part concludes with a recommended publicity right model.

II. RIGHT TO PRIVACY IN INDIA

In India, the right to privacy originates from the common law right of every individual to prevent public intrusion into his private and family life, his home, and his correspondence. Any violation of one’s privacy constitutes a tort and the victim may seek remedy under common law.

The common law in the U.K. does not recognize the right of privacy as an independent right. The violation of privacy must be established through the existing principles of the breach of confidence that flow from a contractual relationship between the parties. However, in the U.S.A., the law recognizes an independent tort of invasion of privacy. There, it is considered a common law

7. See RESTATEMENT (SECOND) OF TORTS § 652(B) (stating that “[o]ne who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person”).
violation of the right if one abuses or misuses another’s personality. Under U.S. law, four wrongs are recognized to constitute invasion of privacy:

i. the intrusion upon one’s physical solitude or seclusion;
ii. Public disclosure of embarrassing private facts of a person;
iii. False Light i.e., putting a person in a false, but not necessarily defamatory position in the public eye; and
iv. Appropriation of some element of one’s personality for a commercial use.

Under Indian common law, when a person is exposed to unwanted publicity without consent and without sufficient public interest, a violation of privacy occurs. The victim may bring an action in a court of law for a preventive order against the continuance of the violation, and also may seek damages for any loss suffered. State actions originated as obvious exceptions to the common law right ‘to be let alone,’ because under common law, most State actions are seen as general exceptions.

The necessity to raise the status of the right to privacy from common law to a constitutional right arose in *Kharak Singh v. State of Uttar Pradesh*, where the Uttar Pradesh Police Regulations allowed blatant intrusions into the private lives of civilians. In considering the constitutional validity of such regulations for the first time, the Supreme Court of India held that the right to privacy flows from ‘Right to Life and Personal Liberty’ enshrined under Article 21 of the Constitution of India. Thus, without a procedure established by law, States cannot take away the rights of an individual. The Court, borrowing heavily from U.S. jurisprudence in *Wolf v. Colorado*, stated that the security of one’s privacy against the arbitrary intrusion by the police is the basis to a free society. India’s Supreme Court further held that right to life did not entail mere animal existence, but instead a right to live with human dignity. According to the Court, the right of personal liberty ensured such human dignity as envisaged under the preamble of the constitution, which is designated to ‘assure dignity of an individual.’ While the common law right to privacy provides remedy against intrusions by private individuals, protection against unreasonable intervention

---

8. *Id.* at § 652(C) (stating that “[o]ne who appropriates to his own use or benefit the name or likeness of another is subject to liability to the other for invasion of his privacy”).
9. *Id.* at 652(B).
10. *Id.* at 652(D).
11. *Id.* at 652(E).
12. *Id.* at 652(C).
14. See U.S. CONST. amend. IV, XIV (stating that “no person shall be deprived of life, liberty, or property”).
into a person’s private life by the State is secured by the fundamental right to privacy recognized under ‘Right to Life and Personal Liberty,’ enshrined in the Indian Constitution.

The Apex Court had the opportunity to reiterate the same principles in *Gobind v. State of Madhya Pradesh and Anr.*, where, in a similar set of circumstances, the court held that privacy rights are to be treated with care and may be compromised only where they conflict with an important superior interest.  

The court observed:

Any right to privacy must encompass and protect the personal intimacies of the home, the family marriage, motherhood, procreation and child rearing. This catalogue approach to the question is obviously not as instructive as it does not give analytical picture of those distinctive characteristics of the right of privacy. Perhaps, the only suggestion that can be offered as unifying principle underlying the concept has been the assertion that a claimed right must be a fundamental right implicit in the concept of ordered liberty.

In another case, *R. Rajagopal v. State of Tamil Nadu*, the Apex Court revisited the fundamental right to privacy, and stated that a State cannot take away the privacy of an individual without a procedure established by law. Further, that procedure must be reasonable and not arbitrary. The court in *Rajagopal* discussed the right of ‘public figures’ to prevent the general public and media from publicizing their views and conduct. It observed that: public figures play an influential role in ordering society, a citizen has a legitimate and substantial interest in the conduct of public figures, and that freedom of press extends to uninhibited debate about the involvement of public figures in public issues and events.

Since *Rajagopal*, courts have shown reluctance to extend the scope of the right to privacy to prevent the general public from knowing about the public appearances of popular characters. The Delhi High Court, in *Indu Jain v. Forbes Incorporated*, observed that:

[C]haracters may be said, of their own volition, to have dedicated to the public the right of any fair portrayal of themselves. One who engages in public affairs and public life to an extent which draws the public interest upon him may be deemed to have consented to the publication of his picture.

In *Indu Jain*, the court endorsed the position in the U.S.A., and emphasised that any violation of privacy is exempted under the right of free speech and expression if the person in question has, of his own accord, waived a right of

18. *Id.* ¶ 24.
privacy by virtue of his public life. The exception for free speech and expression, however, cannot extend to intrusions into one’s private life if he chooses to keep it confidential. The question of interface between the fundamental right to free speech and the fundamental right to privacy requires no elaboration because, under the Constitution of India, fundamental rights are enforceable only against the State.

The privacy exception for famous persons or public characters (‘celebrities’), however, is not absolute and has its limitations. In Phoolan Devi v. Shekhar Kapoor and Orts., the Delhi High Court categorically ruled that the right to privacy must encompass and protect the personal intimacies of the home, family, marriage, motherhood, procreation and child rearing, irrespective of whether the person is a public figure. A celebrity’s right to privacy is rendered infructuous with respect to information that meets the following conditions: (1) The general public should have a legitimate interest in the information, (2) The information should not relate to the celebrity’s private life, and (3) There should be no commercial motives involved in dealing with such information.

The common law in India has always looked at the right of privacy as a negative right - an in rem right to prevent others from invading one’s privacy. The fundamental right to privacy is also a negative right that bars the State from invading one’s privacy except under reasonable legal procedure. A person may, however, contractually waive his common law right to privacy and allow the distinct traits of his persona to be made public for commercial advantage. This right of waiver of the privacy right may be termed ‘right of publicity,’ and has been recognized by courts in India.

The government has taken certain legislative measures regarding privacy to cater to the advancement of communication technology and the advent of the internet and mobile media. The Information Technology Act was enacted to accommodate electronic transactions under the purview of law. Strong provisions have been incorporated in the law to restrict the State’s power to intercept private transactions. Breach of confidentiality and privacy by obtaining electronic information of a person without consent has been made an

23. Section 69, Information Technology Act, 2000 (No. 21 of 2000) “69. Directions of Controller to a subscriber to extend facilities to decrypt information- (1) If the Controller is satisfied that it is necessary or expedient so to do in the interest of the sovereignty or integrity of India, the security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence, for reasons to be recorded in writing, by order, direct any agency of the Government to intercept any information transmitted through any computer resource. (2) The subscriber or any person in charge of the computer resource shall, when called upon by any agency which has been directed under sub-section (1), extend all facilities and technical assistance to decrypt the information. (3) The subscriber or any person who fails to assist the agency referred to in sub-section (2) shall be punished with an imprisonment for a term which may extend to seven years.”
offense punishable by imprisonment. Recently, the Ministry of Communication and Information Technology released Draft Rules on Reasonable Security Practices and Procedures and Sensitive Personal Information, under which corporate entities are restricted from dealing with sensitive personal information, such as passwords, biometric and medical information, user details entered during registration, financial records, etc. The Legislative Department of the Parliament of India has also recently proposed the Right to Privacy Bill, 2011, which is expected to be introduced in the Parliament this year. The Bill aims to provide statutory recognition to the right of privacy and to regulate the collection, use, maintenance, and dissemination of a person’s sensitive information. The Bill also proposes penal action against acts that violate privacy, such as data and identity theft, unauthorized interception, and disclosure of personal, health and sensitive data. The Bill, however, does not mention publicity rights and provides no remedy for false endorsement or use of a person’s identity for commercial purposes.

Despite a few statutory measures, the legal approach to privacy issues in India has been restrictive, and legislators have limited the notion of privacy to only the modalities of one’s private life and personal information. Unlike U.S. law, Indian codified law provides little basis under the principles of privacy for actions against false negative publicity and appropriation of one’s personal traits for commercial benefit. The inadequacy of protection accorded by the traditional principles of defamation and misappropriation necessitated the courts to extend the common law principle of privacy to fill this void.

III. RIGHT OF PUBLICITY IN INDIA

The right of publicity in India is rooted in common law and there is no statute governing the issue. It has evolved from the right of privacy and attaches to an individual or in any indicia of an individual’s personality, such as name, personality trait, signature, voice, etc. A person may acquire the right of publicity by virtue of his association with an event, sport, movie, or any other activity.

24. Section 72, Information Technology Act, 2000 (No. 21 of 2000) “72. Penalty for breach of confidentiality and privacy- Save as otherwise provided in this Act or any other law for the time being in force, any person who, in pursuance of any of the powers conferred under this Act, rules or regulations made thereunder, has secured access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned discloses such electronic record, book, register, correspondence, information, document or other material to any other person shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.”


To possess the right of publicity, a person must be well-recognized among the general public in such a manner that the public can identify the person based on one or more aspects of his persona. By virtue of acquiring publicity rights, a person then acquires the right to prevent commercial use of his persona without permission. Publicity rights will be considered misappropriated if the person’s persona or identity is used in an unauthorized manner for commercial benefit. Despite the existence of publicity rights, a person cannot curtail another person’s freedom of speech and expression. Activities such as caricature, lampooning, and parody, all of which qualify as free expression, are permitted and are not considered a violation of publicity rights. Determining that a publicity right violation has occurred under Indian law requires the following findings: (1) Determination of public recognition or popularity of an individual, (2) Use of such person’s persona for commercial purposes without authorization and (3) Determination of whether the use amounts to parody, lampooning or any other form of permitted free speech and expression.

In India, companies and other legal “persons” do not have the right of publicity. The right attaches only in natural persons. There are very few cases that have expounded the meaning and scope of India’s right of publicity.

A. D.M. Entertainment v. Baby Gift House and Ors.28

Daler Mehndi is a popular music composer, lyricist and singer in India. He was involved in the creation of numerous music albums such as Bolo ta ra ra ra, Dardi rab rab, and others that have been sold extensively across the world.29 In 1996, Mehndi incorporated D.M. Entertainment, where “D.M.” stands for the initials of his name.30 The company was originally created to manage Mehndi’s advancing career and to help raise funds for charities and causes, such as the DALER MEHNDI GREEN DRIVE project.31 After incorporating, Mehndi assigned all his publicity rights, including commercial endorsements and other related rights, to the company.

Baby Gift House (BGH), is a company that owns toy and gift shops throughout Delhi. It sold dolls that were allegedly imitations of, and identical to, the likeness of Daler Mehndi.32 In addition to having Daler Mehndi’s features, the dolls could make moves and sing lines from some of his compositions.33

Aggrieved by BGH’s activities, D.M. Entertainment sued in Delhi High Court, alleging that the importation and sale of the dolls or images were a blatant infringement of Daler Mehndi’s right to control the commercial exploitation of

29. Id. at ¶ 4.
30. Id. at ¶ 2.
31. Id.
32. Id. at ¶ 9.
33. Id.
his persona. The company also claimed that the defendants were liable for false endorsement and passing off, and thus sought a permanent injunction against the defendants.

The Delhi High Court held the defendants liable for violating Mehndi’s right of publicity, for false endorsement, and for passing off. The court granted the permanent injunction and awarded Mehndi token damages. The decision was delivered ex parte because the defendants did not contest the plaintiff’s case.

In deciding the case, the Court analyzed the facts and agreed that Mehndi was a famous and popular personality in India. It considered awards received by the artist, album sales, and other materials in reaching its conclusion. In the high court’s view, Daler Mehndi was extremely famous and precipitated an instinctive association in the public’s mind and trade alike because of the high quality entertainment services and products he created. Therefore, according to the court, his persona had assumed tremendous significance as a quasi-property right, meant to protect the economic value associated with his identity.

With respect to appropriation of Mehndi’s persona, the high court stated that the character and features of Mehndi had been incorporated into the toys. The toys exhibited features, voice, and moves that were characteristic of Mehndi. The Delhi High Court noted that Mehndi’s identity was fused into the toys with the objective of commercial gain. The high court determined that the defendants sold the dolls and thus exploited Mehndi’s publicity value or goodwill of the artist’s persona in the product. Therefore, because Daler Mehndi’s celebrity persona was copied by a commercial product without authorization, the high court concluded that Daler Mehndi’s right of publicity had been infringed.

The Court further noted that the right of publicity can, in a jurisprudential sense, be located within the individual’s right and autonomy to permit or prohibit the commercial exploitation of his likeness or some attributes of his personality. However, the Court noted that in a free and democratic society where every individual’s right to free speech is assured, over-emphasizing a famous person’s publicity rights tends to chill the exercise of such an invaluable democratic right. Thus, caricature, lampooning, parodies, and the like, that tend to mimic aspects of the individual’s personality traits, might not constitute

34. D.M. Entertainment v. Baby Gift House and Ors., High Court of Delhi (Apr. 29, 2010).
35. Id. at ¶ 1.
36. Id. at ¶¶ 3-6.
37. Id.
38. Id. at ¶ 6.
39. Id. at ¶ 13.
41. Id.
42. Id. at ¶ 14.
43. Id.
infringement of an individual’s right to publicity.\textsuperscript{44} The high court pointed out that such protected speech may be expressed in a variety of ways - i.e. cartoons in newspapers, mime, theatre, films, and songs. These forms of expression, in the Delhi High Court’s view, cannot \textit{per se} be held to amount to commercial exploitation.\textsuperscript{45} However, if an individual can demonstrate that the form of expression defames or disparages him, that individual may still obtain damages for libel or slander.\textsuperscript{46}

The Delhi High Court stated that an individual claiming false endorsement must prove that the use of his identity likely misled consumers into believing that he endorsed the product at issue.\textsuperscript{47} In the high court’s opinion, the use of Mr. Mehndi’s persona in conjunction with a commercial product was not proper or legitimate; it amounted to a clear dilution of uniqueness of his personality and gave rise to a false belief that he had either licensed it or that the Defendants had some business connection with the plaintiff that permitted use of his exclusive right to market his own images.\textsuperscript{48} Thus, the Court concluded that the defendants were liable for false endorsement.

A common law action for passing off arises where one person holds out his goods or services to be that of another person in order to benefit from such other person’s good will. To succeed in an action for passing off the plaintiff has to prove (1) the goodwill enjoyed by him, (2) misrepresentation by the defendant, and (3) resultant damage to the plaintiff’s goodwill. The Delhi High Court concluded, observing that in a passing off action, it is for a court to determine whether the defendant is selling goods or services designed or calculated to lead purchasers to believe that they have originated from the plaintiff.\textsuperscript{49} The court stated that such actions might damage the plaintiff’s trademark by reducing or diluting the trademark’s power to indicate its source, even though the defendant might have used the well-known trademark for goods or services that are not similar to those provided by the plaintiff and does not otherwise cause confusion among consumers. According to the high court, even if such dilution might not cause consumer confusion, but takes advantage of the goodwill of the well-known trademark, such conduct constitutes an act of unfair competition.\textsuperscript{50} Because D. M. Entertainment suffered a loss of business, goodwill, and reputation as a result of BGH’s sale of the dolls, the court also held the defendants liable for passing off.\textsuperscript{51}

The \textit{D.M. Entertainment} case is the first case in India to comprehensively expound on the facets of the right of publicity. In addition to establishing the

\textsuperscript{44} Id.  
\textsuperscript{45} Id.  
\textsuperscript{46} D.M. Entertainment v. Baby Gift House and Ors., High Court of Delhi (Apr. 29, 2010).  
\textsuperscript{47} Id. at ¶ 15.  
\textsuperscript{48} Id.  
\textsuperscript{49} Id. at ¶ 16.  
\textsuperscript{50} Id.  
\textsuperscript{51} Id. at ¶ 17.
elements of the right and its violation, the court also noted the applicability of the tort of passing off to publicity. The fame of a celebrity was used by the court as the basis for deciding on the famous-ness of the mark and its passing off. The high court expanded the right of passing off in this case beyond names to other traits of a celebrity’s personality.

Similarly, trademark law in India recognizes the rights of celebrities to prevent use of trademarks that are aimed at taking advantage of the celebrity’s identity. Section 14 of the Trademarks Act of 1999 provides that a trademark that falsely suggests a connection with a living or dead person cannot be registered.52 The provision mandates the acquisition of consent from a person or his descendants in order to register the trademark.53 The objective of the provision is to prevent consumer deception and misrepresentation with respect to celebrity association with the goods or services to which the mark is applied. The Act also recognizes the use of personal names as a valid defense to trademark infringement.54

Although Section 14’s language is not limited to names, and may be extended to identity, the emphasis of other provisions and court judgments has primarily been on names. Names of celebrities have been recognized as distinctive, famous, and said to be on a higher pedestal under the Indian trademark law than well-known marks.55 Using a celebrity’s name as a trademark for any business has been considered likely to deceive the public, and therefore constitutes passing off.56 However, many scholars are questioning whether a celebrity’s personal traits or other identifying attributes are trademarks like names. Such an approach seems inconsistent with well-established trademark jurisprudence, which assesses passing off based on the association or goodwill of a mark with respect to goods or services, rather than on persons and misrepresentation in the course of trade. While it seems plausible to apply the

52. Section 14, The Trademarks Act of 1999. "14. Use of names and representations of living persons or persons recently dead. Where an application is made for the registration of a trademark which falsely suggests a connection with any living person, or a person whose death took place within twenty years prior to the date of application for registration of the trademark, the Registrar may, before he proceeds with the application, require the applicant to furnish him with the consent in writing of such living person or, as the case may be, of the legal representative of the deceased person to the connection appearing on the trademark, and may refuse to proceed with the application unless the applicant furnishes the registrar with such consent."

53. Id.

54. Section 35, The Trademarks Act of 1999. “35. Saving for Use of Name, Address or Description of Goods or Services- Nothing in this Act shall entitle the proprietor or a registered user of a registered trademark to interfere with any bona fide use by a person of his own name or that of his place of business, or of the name, or of the name of the place of business, of any of his predecessors in business, or the use by any person of any bona fide description of the character or quality of his goods or services.”


56. Id.
tort of passing off with the celebrity’s right of publicity as the basis, the trademark approach adopted in Daler Mehndi’s case seems far-fetched.

B. Miss. Kajal Aggarwal v. The Managing Director, M/s. V.V.D. & Sons\textsuperscript{57}

Kajal Aggarwal is a popular film actress in India. She rose to prominence through performances in Telugu movies, such as \textit{Magadheera}, \textit{Brindavanam}, \textit{Mr. Perfect}, and \textit{Darling}. She also acted in a few Bollywood movies. In 2008, Kajal signed an agreement with M/s. V.V.D. & Sons to endorse hair oil and coconut oil products.\textsuperscript{58} The agreement allowed use of Kajal’s profile in photographs, videos, print, internet, and other media to promote the products for one year.\textsuperscript{59} M/s. V.V.D. & Sons continued to use the videos and photographs after the expiration of the agreement, and Kajal filed suit before the Madras High Court, seeking an injunction and damages.\textsuperscript{60}

After reviewing the agreement and hearing arguments, the high court judge held that M/s. V.V.D. & Sons had the right to use the video film for promoting the products because it held copyrights for the work.\textsuperscript{61} However, with respect to the photographs and other profile material of Kajal, the judge delivered an interim order prohibiting their use in print, internet, and other media.\textsuperscript{62} Aggrieved by the order, Kajal appealed to the Division Bench.

The Division Bench agreed with the high court regarding M/s. V.V.D. & Sons’ copyrights for the videos, but noted that copyright ownership does not permit the company to use the video for advertising or promotional purposes.\textsuperscript{63} The court also noted that M/s. V.V.D. & Sons did not have any right to use Kajal’s persona for any advertising or promotional purposes because it could injure her publicity rights and reputation.\textsuperscript{64} According to the Division Bench, M/s. V.V.D. & Sons’ use of Kajal’s persona was likely to cause confusion among the public, which would have a direct impact on Kajal’s advertising and endorsement prospects.\textsuperscript{65}

With respect to Kajal’s application for an interim injunction, the court stated that irreparable harm would be caused to Kajal if the interim order was not passed because it was difficult to assess damages caused to her.\textsuperscript{66} As balance of

\begin{itemize}
\item \textsuperscript{57} Miss. Kajal Aggarwal v. The Managing Director, M/s. V.V.D. & Sons P. Ltd., High Court of Madras (Dec. 22, 2011).
\item \textsuperscript{58} \textit{Id.} at ¶ 2.
\item \textsuperscript{59} \textit{Id.}
\item \textsuperscript{60} \textit{Id.}
\item \textsuperscript{61} \textit{Id.} at ¶ 4.
\item \textsuperscript{62} \textit{Id.}
\item \textsuperscript{63} Miss. Kajal Aggarwal v. The Managing Director, M/s. V.V.D. & Sons P. Ltd., High Court of Madras, at ¶ 22 (Dec. 22, 2011).
\item \textsuperscript{64} \textit{Id.}
\item \textsuperscript{65} \textit{Id.}
\item \textsuperscript{66} \textit{Id.} at ¶ 22.
\end{itemize}
convenience was also in Kajal’s favor, the Court granted an interim injunction against the use of her persona for promotion of the Respondent’s products.67

The Division Bench in Kajal’s case differentiated between the copyright and publicity rights of a celebrity. It held that ownership of copyright in a work does not give the right to use the work for commercial purposes if a celebrity’s publicity rights will be infringed by that use. The court reiterated that the use of a celebrity’s profile for advertising or promotion may only be done after obtaining appropriate authorization.

C. ICC Development (International) v. Arvee Enterprises and Anr.68

ICC Development (International) Limited (“ICC”) organizes cricket tournaments, and was the organizer of the ICC World Cup held in South Africa, Zimbabwe, and Kenya from February 8, 2003, until March 23, 2003.69 ICC created a distinctive logo and mascot for the tournament, and filed registration applications for its trademark in several countries.70 In India, ICC filed applications for registration of “ICC Cricket World Cup South Africa 2003,” its logo, and the mascot. Philips India Limited and its authorized dealers started a campaign to promote their own products by offering tickets to the World Cup.71 It used the slogans “Philips: Diwali Manaao World Cup Jao” (meaning “celebrate the festival of Diwali, go to World Cup”) and “Buy a Philips Audio System to win a ticket to the World Cup.”72 Phillips’s promotional materials showed a pictorial representation of a ticket with an imaginative seat and gate number noting “Cricket World Cup 2003.”73

Aggrieved by Phillip’s actions, ICC filed a suit alleging violation of its publicity rights, among other claims, and sought an interim injunction.74 After the hearing on the injunction, the court opined that, for several reasons, non-living entities were not entitled to the protection of publicity rights in an event.75 First, according to the court, the copyright, trademark, dilution, and unfair competition law provided full protection against all forms of appropriation of property. Secondly, the court stated that such a ruling would be against the basic concept of “persona,” which refers to an individual human being.76 According to the court, the right of publicity evolved from the right of privacy and can only attach to an individual or indicia of an individual’s personality, like his name,

67. Id.
68. ICC Development (International) v. Arvee Enterprises and Anr., 2003 (26) PTC 245 (Del).
69. Id. at ¶ 2.
70. Id.
71. Id. at ¶ 1.
72. Id.
73. Id.
74. ICC Development (International) v. Arvee Enterprises and Anr., 2003 (26) PTC 245 (Del).
75. Id. at ¶ 13.
76. Id.
personality trait, signature, voice, etc. While an individual might acquire the right of publicity by virtue of his association with an event, sport, or movie, the right of publicity cannot attach to the event that made the individual famous, nor in the corporation that organized the event.

The court further stated that any effort to transfer the right of publicity from an individual to the organizer (non-human entity) of the event would be a violation of the Indian Constitution’s Article 19, the Right to Freedom of Speech and Expression, and Article 21, Right to Life. The court further pointed out that no persona can be monopolized because the right of publicity vests in an individual, and he or she alone is entitled to profit from it. For example, if an entity used Kapil Dev or Sachin Tendulkar’s name/persona/indicia in connection with the ‘World Cup’ without their authorization, the players would, according to the court, have a valid and enforceable cause of action. While concluding that publicity rights can exist only in natural persons, the Court referred to U.S. statutes and cases.

To summarize, the right of publicity in India is based in common law and is still evolving. Although courts are clear about the basic elements of the right, confusion still exists regarding the scope of its applicability and enforceability. It is, however, well accepted that the right of publicity cannot restrict free expression, a fundamental right guaranteed by the Constitution of India. Furthermore, courts have stated that the publicity right is a personal – not commercial – right that cannot be possessed by corporations. Nevertheless, a celebrity can assign or license his or her persona to a business entity. Publicity rights infringement, false endorsement, and passing off have been recognized as valid actions for enforcing celebrities’ rights.

Because publicity rights law is only a recent development in India, many Indian celebrities have been relying on trademark and copyright law to protect their publicity interests. Some celebrities who have acquired trademark protection include former Miss World Aishwarya Rai, leading actor Shah Rukh Khan, actress Kajol, spiritual guru Baba Ram Dev, and celebrity cook Sanjiv Kapoor.

In addition to trademarks, Indian celebrities have also been relying on copyright protection to prevent unauthorized commercial use of their persona. However, because the protection afforded by copyright law is limited, a need for a well-defined law of publicity rights is continually urged by celebrities and scholars. Although a few court decisions have recognized publicity rights and expounded on their meaning, ambiguities remain regarding the scope and extent of these rights.

77. Id. at ¶ 14.
78. Id.
79. Id.
80. ICC Development (International) v. Arvee Enterprises and Anr., 2003 (26) PTC 245 (Del).
IV. PUBLICITY RIGHTS AND COMPUTER GAMES

Because the concept of publicity rights is a recent development in India, Courts have had no opportunity to delve into the application of computer games and the virtual world. Therefore, the following hypothetical example will be used to test whether the existing legal framework of the right of publicity, and the premise on which it is based, is broad enough to embrace the challenges posed by the changing landscape of technology and media.

A. Sachin Tendulkar and Others v. FB Sports (a hypothetical case)

A company called FB Sports, headquartered at Bangalore, India, develops a cricket game entitled Sachin Cricket that can be played on computers and mobile phones. FB Sports also develops an online version of the game to facilitate collaborative gaming over the internet. Sachin Cricket has two versions. The first is ‘World Cricket,’ which is played between different countries. Each country has a list of twenty players whose names and identities are very similar to real-life players. A gamer can choose any country and eleven players and play a match. The players’ behaviour and mannerisms are similar to real individuals but the outcome of the game depends on how the gamer plays.

The second version of the game is ‘Premier League,’ which is based on club cricket and is played online. In this version, a gamer can create his own club and bid for players by paying real money for each player in the game. The price of the players is based on the real-life popularity of each player and the player’s financial value changes based on performance. The financial value of the club increases based on its performance in matches played by the gamer, and the players or club can be sold to other gamers. A gamer also has the option to purchase an upgraded avatar of a player. In this format, a gamer does not have the option to change player attributes, such as appearance, behaviour or statistics, which are based on real-life performances. The gamer can also sign endorsement deals on behalf of his players or club for advertisements to be displayed while matches are being played online, and charge real money for the same. All gamers have the option of selling tickets for their matches directly or through FB sports. Fifty-percent of the endorsement and ticket revenues goes to FB Sports. All matches can be recorded and viewed anytime. Gamers can upload the videos on the internet and/or sell them for a price.

Given the popularity of the game in cricket-playing nations such as India, Australia, United Kingdom, and South Africa, Sachin Cricket becomes very popular. The Premier League version of Sachin Cricket becomes a great success, and FB sports earns more than one-hundred million dollars during the first year of its launch. Some gamers also earn revenues exceeding one-million dollars from online advertisements and sale of their virtual clubs and tickets. After noticing the success of the game and receiving no response to their letters from FB Sports, popular cricketers such as Sachin Tendulkar and other Indian cricket players file a case against FB Sports before the Delhi High Court,
alleging violation of their publicity rights and passing off. Most of them, including Sachin Tendulkar, have registered trademarks on their names for business management, consulting, and advertising services.

The issues before the court are as follows:

I. Is FB Sports liable for violating publicity rights of Sachin Tendulkar for using his name for the game?

II. Is FB Sports liable for passing off the game with Sachin’s name?

III. Is FB Sports liable for violating publicity rights of players in the Indian cricket team for including their names and identities in World Cup and Premier League?

IV. Is FB Sports liable for false endorsement and passing off for using the names and identities of players in the Indian Cricket team in Sachin Cricket?

Analysis of the Issues

B. Issue I: Violation of Publicity Rights for Using Sachin Tendulkar’s Name.

As recognized by the High Court of Delhi in Daler Mehndi’s case, a celebrity has the right to control the commercial exploitation of the goodwill associated with his persona. The following factors are relevant to determine whether publicity right of a person is violated:

a. Whether the person is a celebrity by virtue of his popularity;

b. Whether the alleged usage of such person’s identity is for commercial advantage; and

c. Whether the usage is covered under any recognised exceptions.

Here, Sachin Tendulkar is an extremely popular sports person, and his name has enormous goodwill associated with the game of cricket. Secondly, FB Sports is distributing the cricket game “Sachin Cricket” for consideration fee and has developed multiple streams of revenue generation through the online version of the game. Third, the usage of the name in the title of the product does not amount to parody, lampooning, or free expression. Therefore, under the existing law, FB Sports will be held liable for violating the publicity rights of Sachin Tendulkar.

C. Issue II: Liability for Passing Off of Goods under Sachin Tendulkar’s Name.

Indian law permits registration of a celebrity’s name as a trademark. Any unauthorized use of the mark for selling goods or services that leads the purchasers to believe that such goods or services are associated with the celebrity amounts to passing off. In addition, the Delhi High Court has ruled that a celebrity’s popularity may be attributed to his trademark, and that trademark
may be recognized as a well-known mark. In these cases, although the name is used in relation with a different set of goods/services, there may be dilution of the goodwill and famousness of the celebrity’s trademark.

Sachin Tendulkar has a registered trademark in relation to business and management services. Any usage of the name ‘Sachin’ in association with a cricket related product will entail association of the product with Sachin Tendulkar. Although the computer games sold by FB Sports might not infringe on Sachin’s trademark based on similarity of goods or services, because Sachin is a well-known personality and his popularity is transferable to his trademark, the usage of his name by FB Sports might dilute the recognition of the mark and would thus result in passing off.

D. Issue III: Violation of Publicity Rights of Players of the Indian Cricket Team.

Any unauthorized usage of a celebrity’s identity - the name, appearance, mannerism, or any other traits of persona - amounts to a violation of publicity rights if the usage is made for commercial advantage. To identify a publicity rights violation of other players on the Indian cricket team, the same test as discussed in Issue I should be applied.

In the first version of the computer game, World Cricket, all cricket players on the Indian team are famous and well-recognized among the public due to the popularity of the game. They qualify to be celebrities, and thus have publicity rights vested with them. Also, the names and appearances of players are used as part of the game and distribution of the game for valuable consideration amounts to commercial use. However, use of the players’ identities as members of their respective national teams will amount to free expression because no special attributes are provided to each team member and the performance of the players in the game entirely depends on the gamers’ skills. The players and their attributes form part of the expression of the game, rather than being only an element or core of the game. Therefore, this version of the game will not give rise to a publicity right violation because the usage of the persona amounts to free expression.

Conversely, in case of the online version of the game, the Premiere League, FB Sports is exploiting different traits of individual players’ personas. Many instances of using their identity or persona, such as cost for each player, improvement in their attributes, cost based on performance and the option to sell a single player, use a player’s persona as a commodity or good independently, and that usage does not form part of the expression of the game as a whole. The players in this version form the core of commercial exploitation. Therefore, the right of publicity trumps free expression, and hence players of the Indian cricket team will be able to successfully claim a violation of their publicity rights.

According to the Delhi High Court’s decision in Daler Mehndi’s case, if use of a celebrity’s identity is likely to mislead the consumers into believing that the celebrity endorsed the product at issue, then that usage amounts to false endorsement. In the case of the World Cricket version of the game, because most players from cricket-playing nations are included in the game, consumers might not be misled to believe that every player is endorsing the game.

In the online version of the game, however, individual players can endorse brands and be transferred to different teams for a fee. The players in the game behave and play like real-life players and have greater personal attributes attached to them. The likelihood of misleading the consumer is high, and in this scenario, the tort of false endorsement might be extended not only to the online version of the game, but to the endorsement of products by the players in the game.

The Delhi High Court recognized the remedy of passing off where a celebrity’s name is used in association with goods or services without consent. Stated differently, use of a celebrity’s identity in association with goods or services will give rise to an action of passing off because it would amount to misrepresentation in the course of trade, and that would give rise to consumer deception with respect to association with a celebrity. Sachin Cricket uses names and other attributes of the players and players are sold for a price. Also, the game facilitates endorsements and ticket sales while FB Sports receives a portion from the revenues. Through these activities, FB sports is misrepresenting to consumers its association with the cricket players, and would therefore be liable for passing off because such representation will injure the publicity rights of celebrities, resulting in financial loss. Because the Delhi High Court has held that celebrities’ rights stand on a high pedestal under trademark law, the cricketers may also succeed in an action for trademark infringement with the aid of their registered trademarks.

V. Problems with the Existing Legal Framework

The present legal framework surrounding the right of publicity in India is still in the initial stages of development, and therefore poses multiple difficulties in its application. First, the legal status of the right of publicity is unclear because there is no nationwide recognition of the right. Each High Court’s decisions are only persuasive, rather than binding on other High Courts. Therefore, although the Delhi High Court recognized the right of publicity in Daler Mehndi’s case, the Madras High Court, in Kajal Aggarwal’s case, made no reference to the right and decided the case under contract law principles. In the absence of binding precedent by the Indian Supreme Court or statutory provisions conferring the right of publicity, any claim of the right’s violation remains undefined and ambiguous in most states.
Second, courts have recognized free expression as an exception to a publicity violation, but the interface between publicity rights and freedom of expression has not been clearly delineated. There are no objective tests to determine what expression amounts to a violation of the right of publicity and what expressions are protected. While Indian courts have borrowed heavily from U.S. jurisprudence with respect to the evolution of the right of privacy and its subsequent extension to right of publicity, they have yet to delve into the nuances of the interface between privacy, publicity, and free expression.

Lastly, applying the tort of passing off to violations of publicity rights unduly expands the scope of the tort beyond misrepresentation and association with goods or services, as recognized under trademark law. The element of misrepresentation is expanded to include misappropriation, and popularity of a celebrity is placed on equal footing with recognition of consumer association of a mark with goods or services. This expansion transgresses the well-established passing off jurisprudence and brings personal rights into the realm of commercial rights, which the ICC decision sought to keep separate. While this expansion would be beneficial to celebrities, lack of appropriate limitations on the application of the tort might result in liability for legitimate use of a celebrity’s persona.

VI. CONCLUSION AND MODEL FOR INDIA.

Although the Delhi High Court crystallized the elements and exemptions of the right of publicity in Daler Mehndi’s case, the decision has only persuasive value and is not binding in other States. As seen from the Madras High Court decision, courts and judges are not well-informed about the scope of publicity rights. A national law would mitigate the problem. Provisions with respect to publicity rights may be incorporated into the Privacy Bill being proposed by the Indian Government. The bill seeks to give statutory recognition to the right of privacy and make privacy violations a criminal offense and a civil wrong. Although one of the primary objectives of the bill is to protect personal privacy in public life, the bill lacks provisions on publicity rights. Including provisions that address the meaning of a publicity right, instances of misappropriation, exemptions, and remedies in the bill will not only harmonize the law, but will also create uniformity in its application in the various States.

As discussed above, the tort of passing off might not be well-suited for enforcing the right of publicity because it would unduly expand the scope of the tort to include misappropriation. Regardless, the tort is not well-suited to personality rights because they are based on a person’s popularity among the public, while passing off is based on recognition of the origin of goods or services. The distinctiveness of a celebrity’s identity, as rightly recognized by

81. THE RIGHT TO PRIVACY BILL, 2011, Working Draft 3, Legislative Department, Parliament of India
courts, decreases with the celebrity’s increase in popularity, and passing off would not be applicable for non-distinctive association.

Although Indian courts have clearly stated that expression in the form of news, films, songs, and other forms may be exempted from the scope of publicity violation, the test for determining these expressions has not been clearly delineated. The analysis would therefore be very challenging and even more difficult when it comes to rights violations in computer games. The lesson to be learned from U.S. courts is that the line between free expression and infringement of publicity rights is very blurred. U.S. courts have tried various models, ranging from the transformative test to the predominant purpose test, only to learn that the determination is far from certain. The conflicting decisions of U.S. courts are an elucidation of the courts’ troubles.

It is imperative for the Indian courts to learn from U.S. experience and adopt a test that mitigates the uncertainty. In fact, a test based on copyright fair use assessment has been proposed by a U.S. scholar. The test has three factors: (1) the nature of the celebrity’s popularity, (2) the character and purpose of the use of his identity, and (3) the effect of such use on the celebrity. These factors must be balanced in order to reach a decision on a publicity right violation.

This test, with a modification of the last factor to include the interests of the general public, would be very well-suited for India. The last factor should be modified to include the effect of the use on either the celebrity or the public. The test not only ensures that free expression is viewed based on the celebrity’s popularity and how the identity is incorporated, but also encompasses celebrity and consumer interests. By considering various aspects of the use of a celebrity’s rights and the nature of a celebrity’s popularity, the test increases objectivity in the decision-making process, thereby militating against arbitrary results.

The enhanced objectivity would make the test well-suited for computer games and evolving online concepts, which create virtual personalities similar to real-life persons. Although on one hand upholding the need for creative ideas and expressions, the test also ensures that the interests of both celebrities and the public are appropriately protected both on- and offline. Because the test has a strong foundation in copyright law, courts can apply parallels from copyright cases to analyze publicity right violations.

---

82. Andrew M. Jung, *Twittering Away the Right of Publicity: Personality Rights And Celebrity Impersonation on Social Networking Websites*, 86 Chi.-Kent L. Rev. 381.


84. *Id.*

85. *Id.*
A COMPARATIVE REVIEW OF CYBERCRIME LAW AND DIGITAL FORENSICS IN RUSSIA, THE UNITED STATES AND UNDER THE CONVENTION ON CYBERCRIME OF THE COUNCIL OF EUROPE

Galina Borisevich, Natalya Chernyadyeva, Evelina Frolovich, Pavel Pastukhov, Svetlana Polyakova, Olga Dobrovlyanina*
Deborah Griffith Keeling, and Michael M. Losavio**

I. INTRODUCTION

Cybercrime, an aspect of the violation of cyber security, is a matter of international importance. The Internet puts criminals and terrorists worldwide at our electronic doorstep, magnifying security risks and problems. A regime to address cybercrime and cyber security seeks to achieve justice and safety in the distributed, transnational, target-rich environment of world-wide computing. The recent review of the Comprehensive National Cybersecurity Initiative by President Barack Obama, following on work done under the administration of President George W. Bush 1, detailed for implementation concrete steps ranging from situational awareness to deterrence strategies against hostile or malicious actions in cyberspace 2. This extends the earlier concerns of the U.S. 2003 National Strategy to Secure Cyberspace 3, which noted even our homes and families fall under this threat both as target and tool.

This focus on Cybersecurity by the U.S. is paralleled by its concern with threats of transnational organized crime 4.

To address this growing international problem, as of 27-7-2012, thirty-seven countries, including the United States, the United Kingdom, Germany, France

---

* Faculty of Law, Perm State University, Perm, Perm Krai, Russian Federation.
** Department of Justice Administration, University of Louisville, Louisville, Kentucky, U.S.A. Michael Losavio can be reached at: Michael.losavio@louisville.edu.
and Japan, have ratified the Council of Europe’s *Convention on Cybercrime* in an effort to structure a uniform response to increasing cybercrime that ignores national borders. Other high-technology nations – including the Russian Federation, Canada, India, Israel and the People’s Republic of China – have not.

Reflection on the idea of “cybercrime” shows potential problems in analyzing crime involving computers and informatics, particularly new kinds of injury to people in their persons, property and rights. The facts of computer operations may not easily correlate with traditional elements of criminal justice practice. The application of the rules of criminal procedure and evidence must take into account the unique realities of computer use. Addressing cybercrime requires knowledge of computer and network operations and how those operations may differ from usual activities of the processing of information.

Ubiquitous computing extends the risk of cybercrime into nearly all aspects of contemporary activity. Everyday activities may lead to computer misuse, whether from a smart phone, tablet computer, On-board Diagnostics (OBD) automotive computer or bank Automatic Teller Machine (ATM). A cell phone is a high-powered networked computer in the palm of the hand; one study found extensive cell phone use in drug crimes and the presence of cell phone evidence in more than half of violent crimes. Indeed, one narcotics defendant argued that because he did not have a cell phone he could not be a drug dealer (the U.S. Court of Appeals for the Seventh Circuit did not agree.)

The effective administration of justice and promotion of public safety and security in this sphere requires a creative response. The national cybersecurity review in the National Cyber Leap Year Co-Chairs’ Report addressed the need for “game changing” solutions if we are to provide public protection and enforce the law. As both technology and concepts of rights have evolved, criminal law has changed to address misconduct involving new technologies and new injuries as the types of injuries and rights of individuals have changed. Computers can

---


6. An On-board Diagnostics computer monitors virtually every component that can affect emission performance, warns drivers of malfunctions, and stores important information about the detected malfunction so that a repair technician can accurately find and fix the problem. *See, e.g.*, *On-Board Diagnostic II (OBD II) Systems - Fact Sheet / FAQs*, CALIFORNIA ENVIRONMENTAL PROTECTION AGENCY, http://www.arb.ca.gov/msprog/obdprog/obdfaq.htm (last visited May 9, 2012).


9. Mark D. Rasch, *Criminal Law and The Internet in The Internet and Business: A Lawyer’s Guide to the Emerging Legal Issues* (Computer Law Association 1996), ( “In many cases, the use of the computers does not alter the fundamental character of the offense -- bribery
injure others through the use of information, a new means of injury, as well as offering opportunities for old crimes be committed with a new tool. 10 Digital devices make it much, much easier to commit crimes that in earlier times required special skills or resources and were outside the abilities of most people. 11 Some new opportunities for misuse, such as illegal access to a computer, data appropriation and malware coding, are sufficiently unlike traditional crimes that prosecution was difficult or impossible without new sui generis legislation. 12 This has led to new substantive laws to criminalize such conduct and “close the gap”. 13 The full impact of these new laws continues to unfold. To properly review computer misuse as a means of more fully expanding substantive and procedural criminal law, legislators and diplomats must consider several items, including but not limited to:

(1) how various types of misuse may fit in traditional ways within elements of crimes; 14
(2) how computer misuse may fit in new, unexpected ways within elements of existing crimes, requiring special attention to the technical facts of computers and networks; and
(3) how misuse may not fit within the elements of standard crimes, requiring use of new criminal statutes to address the danger.

The intersection of the old and the new with cybercrime makes for an evolving area of practice. Reviewing incidents of computer misuse will require a combination of both traditional and innovative case analysis in law enforcement, especially where the computer crime itself shares elements of old and new types of offenses.

This overview focuses on cybercrime in the context of the American and Russian criminal systems that define crimes through legislative acts and statutes that set out the factual elements of conduct to be punished. American federalism creates a dual system of sovereignty with limited federal criminal jurisdiction. 15 The transnational nature of cybercrime may invokes U.S. federal jurisdiction when actions occur that impact within U.S. territorial jurisdiction or, in some cases, U.S. citizens, although this remains an element of proof in prosecutions. The Russian Federation has general criminal jurisdiction over all cybercrime

---

12. Id.
activity within its jurisdictional sphere.\textsuperscript{16} Prosecution of a cybercrime over a
network may invoke multiple transnational jurisdictions.\textsuperscript{17} The transnational
nature of network cybercrime is a factor that greatly complicates efforts to
address and prosecute these crimes.

The terms cybercrime, computer crime and computer misuse are used
interchangeably. Similarly, we use the terms electronic files, computer files,
electronic documents and electronic evidence interchangeably to refer to the
electronic information created, stored, changed and transmitted by computers
both internally and over networks. This use of computers to store, manipulate
and transmit information gives rise to some key factual differences between
traditional, physical crimes and cybercrime. The U.S. and many foreign
countries have separate statutes for unauthorized access to computers, malware
deployment, illegal interception and other computer offenses. Regardless of the
country of origin, these crimes have the same basic elements as those defined by
American federal law but may differ in scope and penalties. In many instances,
both the scope of activities and punishments may be greater than under U.S. law,
which is a possible reflection of the increasing role of these crimes in everyday
law enforcement. And, in at least one instance, a U.S. state law prohibiting
unauthorized access to a computer was so broad in its definition of illegal
computer usage that it was found unconstitutional.

Computers are used to affect information, but the laws of property relating to
information are very different from those laws of property covering physical
objects. The concept of “\textit{property}” is essential to crimes like theft but is
traditionally grounded in tangible real and chattel property. “\textit{Privacy and
confidentiality}” are important issues regarding the misuse of computer
information. Control of private papers and effects and one’s personal affairs are
part of “privacy,” the invasion of which the law increasingly seeks to protect.\textsuperscript{18}
Computer misuse of information can do great damage to privacy and reputation
in entirely new ways. It is important that legal definitions of property recognize
the significance of this new “property” and its relation to an individual’s right to
privacy and confidentiality.

\textsuperscript{16} See generally, Anton Burkov & Douglas Kramer, \textit{Russian Civil Judicial System,
\textsuperscript{17} See generally, Susan W. Brenner, \textit{Transnational Evidence Gathering and Local
Prosecution of Internet Cybercrime}, & Joseph J. Schwerha IV 20 J. MARSHALL J. COMPUTER &
INFO. L. 347, 376 (2002) (“In addition to acquiring the basic technical knowledge he or she will
need to approach a cybercrime case, the local prosecutor will also have to learn how to obtain
admissible evidence from other jurisdictions, which can be other states or other countries. And
while the process of obtaining evidence from other states can be quite difficult in cybercrime
prosecutions, these difficulties are only compounded when the evidence must be obtained from
another country or countries.”).
Concepts of *dominion, control or possession* are traditionally understood through notions of physical manipulation; however, within the context of cybercrime, dominion and control over a network may involve non-traditional facts that sustain a finding that offenses requiring *dominion, control or possession*. In the “virtual” world, a user acts through the transmission of commands to a computer, whether explicitly typed out or just a click of a button. If those commands give control of a computer or its data, then possession may be established, even from the other side of the world and even if there is not physical control over a physical object. In one transnational computer intrusion case, the trial court found that a computer trespasser’s control of a computer in the United States from a rural region of the Russia Federation over the Internet was sufficient to establish possession of the data and control of the computer.

The administration of justice requires information regarding the facts of any instance of computer misuse meet the following three qualities: (1) the information must match the elements of a crime; (2) the information must be useful under the rules of criminal procedure; and (3) the information must be admissible under the rules of evidence. Unfortunately, the law develops slowly and cautiously while computing technologies evolve rapidly. Computer technological innovation may outrun legal developments for its regulation. Currently, the *definitions* associated with the elements of cybercrimes, particularly network actions, are not clear, consistent or well-defined.

Organized frameworks for criminal statutes help assure completeness, currency and standardization with a regime as well as consistency across jurisdictions. The profound changes wrought by international informatics networks and the transnational nature of crimes involving computing led to the Convention on Cybercrime by the Council of Europe (“Convention on Cybercrime”). The Convention on Cybercrime is a useful, powerful treaty framework for analyzing and conforming national laws regarding cybercrime. It reflects national practices and transnational needs. As a multi-signatory international treaty, it enforces consensus and treaty obligations to conform national cybercrime laws to promote easier enforcement enforceable across borders, reducing the havens for illicit online conduct. It supplements other

---


existing multilateral and bilateral legal assistance agreements and domestic laws relating to criminal law enforcement.22

As of July 27, 2012, thirty-six countries had ratified the Convention.23 An additional fifteen countries had signed but not ratified it, including Canada, South Africa and Sweden.24 Although opened for signature in 2001, the United States did not ratify the treaty until 2006, and Russian Federation is not yet a signatory.25 The People’s Republic of China, Israel and India are not signatories to the Convention.26

The Convention on Cybercrime addresses technical definitions for informatics and computing.27 It also details the core substantive criminal laws required, procedural laws reflecting the special issues with computer and electronic data and evidence and jurisdictional issues that member states must adopted through national law.28 It moves from this substantive and procedural cyber law foundation into principles and rules for international cooperation.29 Countries must implement laws on extradition of suspects and mutual assistance in investigations, including the spontaneous sharing of information on cybercrime between nations and the preservation of electronic evidence.

II. SUBSTANTIVE LAW

The Convention on Cybercrime seeks uniformity of substantive national cybercrime laws.30 Many of the listed offenses, such as computer-related offenses,31 content-related offenses,32 and copyright infringement offenses,33

22. See, e.g., European Convention on Extradition, opened for signature in Paris, on 13 December 1957 (ETS No. 24); European Convention on Mutual Assistance in Criminal Matters, opened for signature in Strasbourg, on 20 April 1959 (ETS No. 30); Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters, opened for signature in Strasbourg, on 17 March 1978 (ETS No. 99); 28 USC §1782. Assistance to foreign and international tribunals and to litigants before such tribunals.
24. Id.
25. Id.
26. Id.
30. Council of Europe Convention on Cybercrime, Chapter III, Section 1, Article 23, Nov. 23, 2001, ETS No. 185.
31. Council of Europe Convention on Cybercrime, Chapter III, Section 1, Title 2, Nov. 23, 2001, ETS No. 185.
32. Council of Europe Convention on Cybercrime, Chapter III, Section 1, Title 3, Nov. 23, 2001, ETS No. 185.
33. Council of Europe Convention on Cybercrime, Chapter III, Section 1, Title 4, Nov. 23, 2001, ETS No. 185.
focus on the computer as the target and tool of the listed offenses, and as only the tool in certain intellectual property crimes.

Additionally, the Convention addresses relatively new offenses against data and systems. These offenses focus on intentional conduct involving devices and data without the legal right to so act. The convention divides such offenses into five categories, which are: (1) access to a computer without or in excess of authorization, (2) interception of data without authorization, (3) interference with data without authorization, (4) interference with a system without authorization, and (5) misuse of devices.

The Convention’s provisions on computer-related offenses relate to computer-related forgery of data and computer-related fraud for economic benefit. These offenses are specifically addressed in the United States Code, and other, more general, fraud-related statues, such as the Wire Fraud Act, apply to computer-related offenses as well.

Content-related offenses under the Convention at this time address only child pornography and the ability to possess, procure, distribute or make available such through a computer system. The Convention prohibition includes visual depictions of a person who: (a) is or appears to be under eighteen years of age or (b) realistic images of a minor engaging in sexually explicit conduct. Signatories may reserve the right not to criminalize simple procurement or possession of child pornography or to criminalize fake images made to resemble minors engaged in explicitly sexual conduct, such as the reservation of the United Kingdom as such a restriction would conflict with

34. Council of Europe Convention on Cybercrime, Chapter II, Section 1, Article 2, Nov. 23, 2001, ETS No. 185.
35. Council of Europe Convention on Cybercrime, Chapter III, Section 1, Title 1, Nov. 23, 2001, ETS No. 185.
36. Council of Europe Convention on Cybercrime, Chapter II, Section 1, Articles 2-6, Nov. 23, 2001, ETS No. 185.
37. Council of Europe Convention on Cybercrime, Chapter II, Section 1, Article 7, Nov. 23, 2001, ETS No. 185. (The computer-related forgery requirement of the Convention appears on its face to be broader than common law forgery of instruments because it deals with the alteration of data with the intent it be acted on. Informatics data is “acted upon” when processed, so alteration of data may do more than simply promote a fraud; it may interfere with system operations. A good example of this is the Stuxnet malware.)
38. Council of Europe Convention on Cybercrime, Chapter II, Section 1, Article 8, Nov. 23, 2001, ETS No. 185.
41. Council of Europe Convention on Cybercrime, Chapter II, Section 1, Article 9, Nov. 23, 2001, ETS No. 185.
42. Council of Europe Convention on Cybercrime, Chapter II, Section 1, Article 9, §§ 2-3, Nov. 23, 2001, ETS No. 185.
43. Council of Europe Convention on Cybercrime, Chapter II, Section 1, Article 9, § 4, Nov. 23, 2001, ETS No. 185.
domestic law regarding indecent photographs of children. An optional protocol prohibiting computer-mediated acts of a racist and xenophobic nature is also available but was removed from the primary treaty due to opposition from the United States that this would conflict with the First Amendment to the U.S. Constitution, a foundational law of the nation.

The explosion of copyright crime made possible by computer and informatics technology, the primary purposes of which are the copying and transmission of data, is addressed in the final substantive law provision of the Convention. Offenses relating to copyright infringement as to literary and artistic works and performances in various media are to be made subject to domestic criminal law with the exception of “moral rights” in copyright. Under the Convention, factors to be considered when criminalizing copyright include that the acts must be committed: (1) willfully, (2) on a commercial scale, and (3) by means of a computer system. The United States and the Russian Federation have criminalized such conduct.

These substantive criminal law provisions must also be met by domestic laws that establish criminal liability for aiding and abetting such crime, for misconduct for corporate entities and appropriate sanctions, including the deprivation of liberty for individuals, that are “...effective, proportionate and dissuasive sanctions.”

III. PROCEDURAL LAW

The procedural law framework of the Convention tackles the special problems presented by transnational cybercrime and the ephemeral nature of electronic evidence. Parties are to set out rules for investigations of any computer-related misconduct and the collection of electronic evidence of all crimes. They may opt out of rules relating to the acquisition of data traffic,
transactional and content information. Though they are encouraged to provide the broadest access to such investigative information, parties are to ensure “adequate protection of human rights and liberties” such as those detailed in the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights and other pertinent treaties. This includes the provision of independent supervision of the exercise of state police power in such investigations, such as judicial oversight.

The Convention directly addresses key technical problems in cybercrime investigations. Those technical issues are primarily derived from the nature of the storage, transmission processes, data processing media and the physical challenges of transnational activity. Effective criminal investigations relating to computer systems require procedures including the following:

1. expedited preservation of stored computer data;
2. expedited preservation and (partial) disclosure of traffic data;
3. procedures and process for the production of stored and subscriber data;
4. procedures for the search and seizure of stored computer data, including assuring the integrity of that data and, where appropriate, expeditiously extending the search across a network;
5. methods to collect, and compel a service provided to assist with, traffic data of computer transmissions;
6. methods to collect, and compel a service provided to assist with, the interception of content information.

These requirements reflect the influence of procedural law on the operational governance of state police power, protections for the rights of citizens and sovereignty.

51. Council of Europe Convention on Cybercrime, Chapter II, Section 1, Article 14, §3 November 23, 2001 ETS No. 185.
52. Id.
53. Council of Europe Convention on Cybercrime, Chapter II, Section 1, Article 15, §1 November 23, 2001 ETS No. 185.
54. Council of Europe Convention on Cybercrime, Chapter II, Section 1, Article 15, §2 November 23, 2001 ETS No. 185.
55. Council of Europe Convention on Cybercrime, Chapter II, Section 1, Article 16, November 23, 2001 ETS No. 185.
56. Council of Europe Convention on Cybercrime, Chapter II, Section 1, Article 17, November 23, 2001 ETS No. 185.
57. Council of Europe Convention on Cybercrime, Chapter II, Section 1, Article 18, November 23, 2001 ETS No. 185.
58. Council of Europe Convention on Cybercrime, Chapter II, Section 1, Article 19, November 23, 2001 ETS No. 185.
59. Council of Europe Convention on Cybercrime, Chapter II, Section 1, Article 20, November 23, 2001 ETS No. 185.
60. Council of Europe Convention on Cybercrime, Chapter II, Section 1, Article 21, November 23, 2001 ETS No. 185.
A. International Cooperation

With harmonization of national laws addressed, the Convention tackles cooperation between nations to pursue computer-related offenses and electronic evidence. This is vital given the ephemeral nature of electronic and digital evidence and its dispersal across wide-area networks that may span the globe. Parties to the Convention agree to cooperate “to the widest extent possible for purposes of investigations or proceedings” relating to computing offenses.61 Parties are to implement procedures to expedite evidence collection and law enforcement cooperation across borders. Law enforcement cooperation between nations not covered by the Convention defaults back to bilateral relations between parties, such as those covered by Multilateral Legal Assistance Treaties.62

Cooperation across borders focuses on: (1) effective extradition of subjects; (2) mutual assistance in investigations; and (3) providing information in support without the need for a request.63 Parties set out their extradition procedures and designate the responsible authority for handling extradition requests between nations, a registry of which is maintained by the Secretary General of the Council of Europe.

Once there is agreement for maximum possible cooperation, the parties should accept expedited requests via media such as encrypted email and responding to them. Parties may decline to offer mutual assistance per local law but should not refuse assistance solely because it considers the matter a fiscal offense. In particular, where a nation whose assistance has been requested requires “dual criminality”, the alleged misconduct is an offense in both the requesting and requested nations. This condition is met if the conduct is an offense under the nation’s laws regardless of terminology, denomination or categorization of the conduct.64 The provision of “spontaneous information” made without a request may be made subject to conditions by the providing Party.

The Convention provides for default procedures for mutual assistance where other international cooperation agreements are not in place, this includes a registry of contact authorities among the party nations.65 Parties may decline to respond for matters considered political offenses or offenses that would

61. Council of Europe Convention on Cybercrime, Chapter II, Section 1, Article 23, November 23, 2001 ETS No. 185.
63. Council of Europe Convention on Cybercrime, Chapter II, Section 1, Articles 24-26, November 23, 2001 ETS No. 185.
64. Council of Europe Convention on Cybercrime, Chapter II, Section 1, Article 25, §§ 1-5, November 23, 2001 ETS No. 185.
65. Council of Europe Convention on Cybercrime, Chapter II, Section 1, Article 27, November 23, 2001 ETS No. 185.
otherwise compromise public order and sovereignty.\textsuperscript{66} Direct judicial requests for assistance may be made in exigent circumstances with notice to the central authorities as well as through the International Criminal Police Organization ("Interpol"). Where assistance is unavailable, the requested authorities should refer the matter to national authorities and notify the requesting party.\textsuperscript{67} Confidentiality or limitations on use of information supplied under mutual assistance may be required by the requested party.\textsuperscript{68}

The unique engineering of electronic systems and digital data create special problems in its investigation, preservation and authentication. The Convention suggests procedures to address those matters. Given how quickly and easily stored computer and electronic data may be destroyed or modified, the Convention provides for requests for expeditious preservation of clearly defined data stored in a computer system within the territory of a request party.\textsuperscript{69} A party may decline this request if its requirements of dual criminality are not met, it deems the matter a political one or it may otherwise impact sovereignty or public order.\textsuperscript{70} Such data preservation should be for a minimum of 60 days.\textsuperscript{71} Where the requested party finds that the data trail includes a service provider in another country, it should expeditiously disclose that and adequate traffic data to trace that data trail to that next node.\textsuperscript{72}

The Convention moves into mutual investigative activities where one party may request another to “search…access, seize…secure and disclose” data stored via a computer system within its territory; expedited responses should be made when provided by implementing law or where there are grounds that the data is at risk of loss, damage or change.\textsuperscript{73} Parties may access publicly available computer data across borders and access data on computer systems with voluntary and lawful authorization across borders without violating sovereignty.\textsuperscript{74} Parties are required to assist in the real-time collection of traffic

\begin{footnotesize}
\begin{enumerate}
\item[66.] Council of Europe Convention on Cybercrime, Chapter II, Section 1, Article 27, § 4, November 23, 2001 ETS No. 185.
\item[67.] Council of Europe Convention on Cybercrime, Chapter II, Section 1, Article 27, § 9, November 23, 2001 ETS No. 185.
\item[68.] Council of Europe Convention on Cybercrime, Chapter II, Section 1, Article 28, November 23, 2001 ETS No. 185.
\item[69.] Council of Europe Convention on Cybercrime, Chapter II, Section 1, Article 29, November 23, 2001 ETS No. 185.
\item[70.] Council of Europe Convention on Cybercrime, Chapter II, Section 1, Article 29 §§ 4-5, November 23, 2001 ETS No. 185.
\item[71.] Council of Europe Convention on Cybercrime, Chapter II, Section 1, Article 28 § 7, November 23, 2001 ETS No. 185.
\item[72.] Council of Europe Convention on Cybercrime, Chapter II, Section 1, Article 30, November 23, 2001 ETS No. 185.
\item[73.] Council of Europe Convention on Cybercrime, Chapter II, Section 1, Article 31, November 23, 2001 ETS No. 185.
\item[74.] Council of Europe Convention on Cybercrime, Chapter II, Section 1, Article 32, November 23, 2001 ETS No. 185.
\end{enumerate}
\end{footnotesize}
data and interception of content data,\textsuperscript{75} often key evidence in criminal investigations. To assure that these obligations for mutual assistance may be effectively implemented, each party nation must designate a point of contact available on a seven day a week, twenty-four hour a day basis to assure responsiveness for such ephemeral activity. This assistance may include technical advice, data preservation, evidence collection, legal advice and locating suspects.\textsuperscript{76}

B. Substantive Cybercrime Laws of the Russian Federation and the United States of America

The cybercrime laws of the Russian Federation and the United States reflect each country’s specific legal and social systems. The Russian Federation gives primacy and general jurisdiction to federal law with limited powers to the administrative regions (such as “Oblast” or “Krai”). In the United States, limited criminal jurisdiction is given to the federal government\textsuperscript{77} and general criminal jurisdiction remains with the fifty states;\textsuperscript{78} however, because the federal government has jurisdiction over interstate and state-foreign commerce, as a practical matter, jurisdiction of much of the misconduct involving computers and networks within the United States remains with the federal government. This jurisdictional connection remains a proof element that must be established at trial or in a plea colloquy.

The early development of computers and informatics focused on improving power and performance. Worries about misuse were minimal as these systems were mostly large, expensive, and operated by government, large businesses and universities.\textsuperscript{79} Controls over misuse were primarily controls over physical access. The evolution of the Internet followed this same pattern. Research scientists at universities and government agencies created a network for the easy exchange of information with other scientists. Information security was an afterthought and of low priority for most activity due to the additional costs it required.\textsuperscript{80} The rapidly evolving telecommunications and Internet technologies have been improving not only the forms of communication, but have opened the gates to new and expanded information and telecommunication crimes.

For both the Russian Federation and the United States, crimes in the sphere of computer information by its nature present a different latency. Those who

\textsuperscript{75} Council of Europe Convention on Cybercrime, Chapter II, Section 1, Articles 33-34, November 23, 2001 ETS No. 185.
\textsuperscript{76} Council of Europe Convention on Cybercrime, Chapter II, Section 1, Article 31, §1, November 23, 2001 ETS No. 185.
\textsuperscript{77} U.S. CONST. art. 1, § 8.
\textsuperscript{78} U.S. CONST. amend. X.
\textsuperscript{80} Id.
commit such offenses can use various technical means of training, commission and concealment of their criminal activities. The technical means include computer facilities, telecommunications, networking equipment and software. All these means help criminals disguise their criminal activity and allow them to avoid prosecution.

Moreover, law enforcement agencies in some cases do not even know about such crimes or have the skills to investigate them. A significant number of computer crimes go undetected not only due to the latency of this type of crime, but also because the activity would not adequately be addressed by the rule of law. Lack of legal regulation is due to the rapid technological growth of information and computerization of the populations of all countries. This caused a break between practice and legal settlement of this scope of practice. The legal vacuum spawned not only organizational, technical, managerial problems in the field of information and telecommunication systems of communication, but also prevented law enforcement agencies of the state from acting against cybercrime. This legal uncertainty is also reflected in the international fight against cybercrime.

The explosive expansion of personal computers and the Internet throughout the world, accompanied by the hypertext features that facilitated use, is now history; with this expansion came tremendous growth in cybercrime. Computer and network security have become major issues for everyone, just as physical security has historically been important for banks, law enforcement and home owners. The lack of security engineering in these systems was like leaving the bank doors open without any bank personnel present. There were new opportunities for misuse directed at how computers work.

Within the Russian Federation, there are some basic organizational and management decisions aimed at resolving the information and telecommunications business in Russia and the related opposition to these types of computer crimes. The new edition of the Federal Law “On Information, Information Technologies and Information Protection” regulates the relations arising from: (1) the right to seek, receive, transfer, production and dissemination of information; (2) the application of information technology; and (3) the protection of information. The Federal Law “On Personal Data” regulates relations connected with the processing of personal data carried out by the Russian federal authorities, state authorities of the Russian Federation and other state bodies, local self-government through the use of data processing.

81. Id.
82. For example, a short list of issues raised by an information security breach are a loss of confidentiality or “theft” of information; damage or modification of information on the system; and a “masquerade” whereby someone, using your system identity, acts in your name.
One of the most important regulations in this area is the Federal Law “On Communication”, which establishes the legal basis of activity in the field of communications in the Russian Federation and under the jurisdiction of the Russian territories. 85 It defines the powers of public authorities in the field of communications, as well as the rights and responsibilities of persons involved in such activities or using communication services. In 2007, the Russian Government adopted the Regulations in the provision of telematic services (telecommunications and information technology processing), designed to establish the relationship between the subscriber or user, on the one hand, and on the other hand, a telecom operator, providing telematic services. The value of these instruments in the first place is that they set not only the legal status of the various stakeholders, but the terminology and technology of information and telecommunication activities necessary for law enforcement to combat crime under a rule of law. Along with creating a legal framework for information and telecommunications activities was the creation of executive agencies in this area, particularly the Ministry of Information Technologies and Communications. 86 In the United States there is less regulation in this sphere, although some has evolved over time. The Electronic Communications Privacy Act, Parts I and II, set out limitations on access and disclosure of user activity generally and as it may relate to computer and network misuse. 87

1. Offenses Against the Confidentiality, Integrity and Availability of Computer Data and Systems

The laws prohibiting unlawful access to a computer and interference with the information a computer processes vary between the two jurisdictions. Both federal U.S. and Russian law leave the definition of unauthorized access to general usage. Other jurisdictions may go into great detail. For example, one American state defines “Access” as set out below.

[‘Access’ means] to approach, instruct, communicate with, manipulate, store data in, retrieve or intercept data from, or otherwise make use of any resources of, (i) any device, equipment, or facility that uses a computer program or other instructions, stored either temporarily or permanently, to perform specific operations including but not limited to logical,

86. The Ministry of Information Technologies and Communications is the main Russian Federation executive branch responsible for public policy and legal regulation of information technology, telecommunications and postal services, including the use of information technology in the formation of state information resources and access to them, the development of television systems and radio, use and conversion of radio frequency spectrum. This Ministry also serves as the communications administrations of the Russian Federation in international activities in the field of communications.
arithmetic, or memory functions with or on data or a computer program that can store, retrieve, alter, or communicate the results of the operations to a person, computer program, computer, computer system, or computer network; (ii) an interconnection of two (2) or more devices used for the purpose of transmitting any combination of voice, video, or data including but not limited to bridges, routers, switches, antennas, or towers connected by hardware or wireless communications lines; or iii) a set of related computer equipment, devices, data, computer programs, procedures, or associated documentation concerned with the operation of a computer or hardware that is designed to perform a specific function.88

This is a broader, more technical and specific definition of the key element of “access” than in the U.S. federal statute.89 Using this more detailed definition, “access” to a computer occurs even when someone walks over and picks up the user guide for a computer or program.

Both the Russian Federation and the United States have core sets of statutes for addressing cybercrime in the context of unauthorized access. Within the Russian Federation, there are the statutes set out in Chapter 28 of the legal code. These are Crimes in the Sphere of Computer Information, Federal Law No. 64-FZ of June 13, 1996, and include: (1) Article 272. Illegal Accessing of Computer Information, (2) Article 273. Creation, Use, and Dissemination of Harmful Computer Viruses, and (3) Article 274. Violation of Rules for the Operation of Computers, Computer Systems, or Their Networks.90 In the United States, the most relevant U.S. statutes are the Computer Fraud and Abuse Act91 combined with additional provisions in the Electronic Communications Privacy Act, Parts I and II.92 In both the Russian Federation and the United States, other statutes also regulate additional aspects of misconduct and investigative practices relating to data, information and computer and network systems.93

2. Unauthorized Access to a Computer

One of the first “new” computer crimes was the illegal use or access to a computer and the information stored within, either directly or over a network.94

92. 18 USC §§ 2510, et. seq.; 18 USC §§ 2701 et. seq.
94. See generally, Robert Flor, Fraud, Computer-related Fraud, and Identity-related Fraud, Criminal Law and Information Technology – Criminal Law & ICT (March 2009), http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-
This is sometimes called “hacking” a computer. The basic elements of illegal access to a computer are: (1) access, (2) to a computer, (3) without authorization or in excess of authorization. Although illegal access to a computer seems akin to the traditional crime of trespass, it does not have the necessary traditional element of physical presence. Traditional criminal trespass was committed by someone “...when he knowingly enters or remains unlawfully in or upon premises” where “A person “enters or remains unlawfully” in or upon premises when he is not privileged or licensed to do so.” But illegal computer access has no such physical entry. It is like placing a telephone call to someone at home; there is interaction via the telephone, but there is no physical entry there. Unauthorized access to a computer prohibitions also protect privacy and confidentiality, which can be violated without a physical intrusion. Unauthorized access invades privacy in ways the law might wish to punish, and in this respect is similar to voyeurism.

Simply put, these new statutes make the use of a computer without permission illegal. The United States and its individual states each have statutes defining unauthorized computer access. These statutes and their individual elements differ from one state jurisdiction to another. What is illegal computer access in one jurisdiction may not be a crime in another.

“Access” to a computer is usually gained through electronic communication of commands and information. This communication could originate from a keyboard attached to a computer, from an attached device, or from another computer over a network. Given the pervasive use of computers in all aspects of modern life, the misuse of computers holds the potential for an increasing number of injuries and wider criminal enforcement. Unauthorized access to a computer can be a crime by itself or may require additional elements of misconduct to be illegal. The illegality of using a computer without permission is similar to the illegality of walking into someone’s home without an invitation,

---

95. The term “hacker” originally referred to a hard working computer aficionado who would work on a computer-related problem and “hack” a solution. People who sought unauthorized access to computer systems, often using purloined passwords that required no real computer skills to exploit, were called “crackers,” as in “safe crackers.” But popular culture latched on to the term “hackers” and the rest is history.


97. The 18 USC § 2511 prohibitions on the interception of electronic communications were amended to permit interception from “computer trespassers” via 18 USC § 2510 (21) where “computer trespasser” -- (A) means a person who accesses a protected computer without authorization and thus has no reasonable expectation of privacy in any communication transmitted to, through, or from the protected computer.


which would likely give rise to criminal and/or civil liability for trespass. Under this logic, following acts could be illegal: (1) using a cellphone without permission; (2) using a wireless Internet access point without permission; (3) using someone else’s computer without permission.

3. The Russian Federation

The Russian Federation (RF) Criminal Code 1996 provided a separate chapter in Section 11, “Crimes in the Sphere of Security and Public Order” called “Crimes in the Sphere of Computer Information.” The chapter begins with Article 272, which outlines the crime of “Illegal Accessing of Computer Information.” The article was included due to the large number of cases of unauthorized access to computer information as part of computer crime due, in part, to: (1) increased access to Internet services through unlimited plans offered by many providers, which increased the latency of crimes; (2) the belief that unauthorized access was infrequently prosecuted; and (3) the termination of a majority of criminal cases during the preliminary investigation and pre-trial stages on the grounds of non-rehabilitation (e.g. reconciliation of the accused with the victim).

Research and analysis on the methods of investigation of unauthorized access to computer information is an urgent issue for several reasons. First, investigation methods impact the identification of the long-term implications of unauthorized access to computer information, particularly the damage to individuals and to society as a whole. Second, analysis of other crimes related to using computer equipment (e.g. Art. 146 of the Criminal Code – violation of copyright and adjusted rights; Art. 183 of the Criminal Code – unlawful gathering and disclosure of information constituting commercial, tax or banking secrecy etc.), which also can be investigated with the techniques of investigating computer crimes. Third, continued research and analysis will help assess the impact of new, high-speed, high-access informational technologies on illegal access to computer information in order to further perfect investigatory techniques. This research will contribute to understanding of the quality of investigations which can help to decrease the latency of such crimes. Analysis

102. По данным Управления Судебного департамента при Верховном Суде РФ по Пермскому краю. Currently, there are court verdicts on only a few cases. In the Perm Region 2009, there were two persons convicted of Art. 272 of the Criminal Code and in 2010 there was only one person accused of a violation of the same article. (Administration of the Judicial Department, Supreme Court of the Russian Federation Perm Krai).
103. Most monographs on the issue were written ten years ago, at the time when distant access was carried out via modem and wires.
of current legislation, court practice and scientific literature shows continuing problems of criminal practice in this area also need resolution.

Information of limited access has a special legal status in the Russian Federation. It is stated by law and therefore is designed for a limited number of persons eligible to know it. The limitations on access to information is determined by federal laws in order to protect the basis of the constitutional order, morality, health, rights and the legitimate interests of other persons, national defense and state security.104

In the Criminal Code of the Russian Federation, as with U.S. law, there is no definition of the term access or unauthorized access, which leads to uncertainty as to the scope of this term and what conduct constitutes its violation. Skuratov and Lebedev assert unauthorized access to computer information means “any form of [unauthorized] penetration into the source of formation with the help of the electronic – calculative equipment, that enables manipulations with the obtained computer information.”105 In April, the Perm Krai Court of Cassation stated that “actually such access is carried out with the help of electronic – calculative equipment and technologies means “breaking into” the electronic system of the defense of the documented information by means of some other name (login), changing addresses, technical devices, modification of software and information provision.”106

The crime of unauthorized access takes the form of active operations, consisting in the unlawful access to and or information resources. Important to the finding of misconduct and guilt is the fact that the person had no right to access the information: to see it, to know it and/or dispose of it. Illegal unauthorized access to computer information has socially dangerous and offensive consequences. These are expressed in the form of destruction, modification or copying computer information, as well as violations of computers, computer systems or networks.

Under the RF Criminal Code, an offender is a competent person liable for the crime if older than 16 years of age at the time of commission of the crime. The mens rea for unauthorized access is deliberate or careless; an offender may commit crimes because of mischief or sport as well as for theft and be prosecuted.107

104. This data can include the data from military, international policy, economic, intelligence, counterintelligence, operational and investigative activity, information pertaining to an individual (last name, first name, year, month, date and place of birth, address, marital status, social and property status, education, profession, income, etc.), and information constituting a commercial secret, information on bank deposit transactions.


106. Дело №22-2026 за 2009 год / Текущий архив Мотовилихинского районного суда г. Перми. Case № 22-2026 of 2009 / The Current Archive of the Motovilikha District Court, Perm.

107. Criminal Code of the Russian Federation, Article 20, §1; Article 24; Article 272.
The Criminal Code of the Russian Federation could benefit from additional definitions relating to conduct such as destruction of information, blocking of information, modification of information, and breaking computers, computer systems and networks. This will help ensure the rights and lawful interests of the individual State, the establishment of uniformity in practice. It should be noted that unauthorized access to computer information has a high latency (in different regions of Russia latency reaches 80%). The reasons for this phenomenon are varied and are described in the legal literature.108

Russian scholars and practitioners understand the “way of commission of the crime” to mean the preparation of the offender for the commission and concealment of crimes, based on objective and subjective factors, and involve the use of appropriate tools and resources. The methods of unauthorized access to computer information are detailed in Russian jurisprudence.109

The Russian Federation Law “on Changes into the Criminal Code of the Russian Federation and Separate Acts of the Russian Federation” on 07.12.2011, in the article 272 of the Code specifies a newly modified notion (definition) of this type of the cybercrime of illegal access. The revised statute now includes the following definition: “Illegal access to law-protected computer information means the action, resulting in destruction, blocking, modification, or copying computer information.”110 This definition clarifies the term “computer information” to include information (messages, data), presented in the form of electric signals, regardless of the means of their storage, processing and transfer. These revisions to the Article 272 of the Criminal Code of the RF will enhance the ability of law enforcement officials to investigate these offenses.


110. УГОЛОВНЫЙ КОДЕКС РОССИЙСКОЙ ФЕДЕРАЦИИ [UK RF] [Criminal Code] art. 272 (Russ.).
4. The United States

The fundamental structure of U.S. law regarding unauthorized access is similar to that of the Russian Federation. States within the U.S. may require additional elements or acts of misconduct to constitute an unauthorized computer access offense. Pointedly, the U.S. statute defines neither “access” nor “authorization,” leaving that to common understanding and interpretation of the term.\textsuperscript{111} It has been suggested that: “The federal computer fraud and abuse statute… shields them from trespassing, threats, damage, espionage, and from being corruptly used as instruments of fraud. It is not a comprehensive provision, instead it fills cracks and gaps in the protection afforded by other state and federal criminal laws.”\textsuperscript{112}

Additional elements define more severe misconduct and increase the severity of punishment for that offense, tying the punishment to the motives of the criminal and the amount and type of damage done. This is analogous with simple trespass usually having a lesser punishment than a trespass intending to commit theft (burglary).\textsuperscript{113} Someone committing unauthorized access to a U.S.-protected computer may receive a greater punishment if for purposes of committing a theft or injury rather than just snooping around. This scheme is seen in the tabular summary of the Computer Fraud and Abuse Act, 18 USC § 1030, the U.S. anti-hacking statute.\textsuperscript{114}

<table>
<thead>
<tr>
<th>Maximum Imprisonment (in years)</th>
<th>Elements of Offenses under 18 USC 1030</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>(a) (2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby <strong>obtains information</strong></td>
</tr>
<tr>
<td>5</td>
<td>(a) (2) &amp; (a) (4) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains certain information for financial or criminal gain, further a tortious act or the value of the information obtained exceeds $5,000, or acts with the intent to defraud</td>
</tr>
<tr>
<td>5</td>
<td>(a) (5) (A) (ii) intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes certain kinds of damage aggregating at least $5,000 in value or creating a risk to personal or public safety.</td>
</tr>
<tr>
<td>10</td>
<td>(a) (5) (A) (i) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, <strong>intentionally causes damage</strong> without authorization, being certain kinds of damage aggregating at least $5,000 in value or creating a risk to personal or public safety.</td>
</tr>
</tbody>
</table>


\textsuperscript{113} In one Model Code jurisdiction, simple trespass is punished with only a fine, but aggravated burglary is punishable by imprisonment from 10 to 20 years. See KY. REV. STAT. ANN. § 511.020 (LexisNexis 2012).

(a) knowingly accessed a computer without authorization or exceeding authorized access, and by means of such conduct having obtained [classified] information with reason to believe that such information so obtained could be used to the injury of the United States, or to the advantage of any foreign nation, [and] willfully communicates or fails to return that information.

Under this model, the U.S. unauthorized access to a computer statute increases the penalty depending on the: (1) purpose of the access, e.g., to facilitate a crime, through recklessness or simple curiosity, and (2) the kind and extent of damage done.\textsuperscript{115} An example under this scheme might be access to someone’s email, Facebook account or wireless access point\textsuperscript{116} without the person’s permission and reading messages from other people. If the intent is only for mere curiosity, this would be a misdemeanor. But if the intent is to send fake hateful emails to damage the person’s reputation, then a felony charge might be possible. And while purpose of access and damage rendered are components of sentence severity, the concepts of “authorization” and “access” are left to the general sense of the words rather than being defined by statute. There is some concern about the potential misuse of overbroad definitions for these terms.\textsuperscript{117} One U.S. jurist called upon a standard dictionary to define “access” as: … the word “access,” in this context, is an active verb: it means “to gain access to,” or “to exercise the freedom or ability to make use of something.”\textsuperscript{118}

Harvesting email addresses of customers in violation of a user agreement\textsuperscript{119} has been found to be a violation of authorized access, while masquerading as a young boy to torment a young girl in violation of user terms against using fake identities was not.\textsuperscript{120}

C. Viruses, Malware, Network Attacks: Injuries from Computer Code

Widespread use of computers has led to misconduct in the form of malicious software programs (“malware”) that interfere with or damage computers and computer data. “Malware” includes computer viruses, computer worms and “Trojan” programs. “Malware” is any program or software designed to interfere

\textsuperscript{116} Hale, Robert V., Wi-Fi Liability: Potential Legal Risks In Accessing And Operating Wireless Internet, 21 SANTA CLARA COMPUTER & HIGH TECH. L.J. 543 (March 2005).
with or damage computer operations, security or information.\textsuperscript{121} A Trojan program masquerades as one type of program but contains software that does something else. Some Trojan programs allow remote control of an infected computer over a network. This can be simply to see what’s on a computer or visible through an attached webcam; it may also be to copy or destroy information on it or use it to launch attacks against other computers. A computer virus is a computer program (a writing) that automatically copies and distributes itself and may interfere with or damage computer operations, security or information. The first such programs were self-replicating and distributed through media like diskettes used first on an infected machine and then on another. The growth in network use, especially the Internet, led to network distribution by e-mail and web sites as an effective method of distribution.

Computer networks have been attacked in several ways. One is the “Denial of Service” (“DoS”) attack where so much network traffic is sent to a computer, like requests for web pages or e-mails, that the computer becomes overloaded and can’t handle legitimate activity.\textsuperscript{122} A web server computer on the Internet would become useless under such an attack.

Prosecuting someone for writing a malware program raises several issues. The destruction of property, whether by terrorist or vandal, is another traditional “physical” crime that has analogous computer misconduct. For example, a person may be guilty of criminal damage to property when “he intentionally or wantonly defaces, destroys or damages any property causing pecuniary loss of $1,000 or more.”\textsuperscript{123} But the actual facts of computer misconduct don’t match well with notions of physical conduct. Proving the malware writer “caused” the damage to a particular computer may be difficult. Simply writing a malware program is not a crime. Placing the malware on one computer may be one crime, but if distributed to other computers without direct action by the malware writer it may be difficult to hold the writer responsible for that greater damage.

Another key issue is that of “property.” If the only result was damage to information, that may or may not constitute damage to “property.” With a Denial of Service attack there is no physical damage to the computer and no damage to the information on it. The computer and its information are just


\textsuperscript{122} A distributed denial of service attack grinds a website to a halt by swamping the computer controlling the website with an overwhelming number of requests that are disguised to look innocuous. See generally Cassell Bryan-Low & David Roman, Spain Arrests Three in Sony Site Attack, WALL ST. J., June 11, 2011, http://online.wsj.com/article/SB10001424052702304259304576377380781996012.html?KEYWORDS=denial+of+service ("Denial of service attacks cause havoc by bombarding websites with data with the aim of knocking them offline."); see also How CloudNine Wound Up in Hell, W IRED (Feb. 1, 2002), http://www.wired.com/techbiz/media/news/2002/02/50171 ("In a DDOS attack, a computer is swamped with an overwhelming number of requests that are disguised to look innocuous, so that the website that it controls grinds to a halt.").

\textsuperscript{123} KY. REV. STAT. ANN. § 512.020 (LexisNexis 2012) (criminal mischief in the first degree).
unavailable for use by those who operate the system and those who want to access it. This interference with possessory interests – a trespass to chattels in U.S. common law – is criminalized by both the Russian Federation and the United States which have addressed this with sui generis statutes prohibiting such conduct.

The Computer Fraud and Abuse Act criminalizes malware attacks. This provision prohibits the knowing transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes certain damage without authorization to “protected” computers, being a federal machine or one connected to the Internet. Damage aggregating at least $5,000 in value or creating certain risks to personal or public safety are covered by the statute. Those threats include: (1) the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals; (2) physical injury to any person; (3) a threat to public health or safety; (4) damage affecting a computer used by or for an entity of the United States Government in furtherance of the administration of justice, national defense, or national security; or (5) damage affecting 10 or more protected computers during any 1-year period.

Similarly, Article 273 of the Criminal Code of the Russian Federation specifically targets the creation, use and dissemination of harmful computer viruses and Article 273 prohibits the creation, use and dissemination of computer viruses or malware that knowingly cause: (1) unauthorized destruction, changes, copying or interference in access to information or (2) interference with computer systems or networks. Depending on the resulting damage or injury, punishment may include imprisonment for up to seven years, although there is no minimum damage amount required for violation of Article 273.

This Russian code article is both narrower and broader than the section added to the U.S. Computer Fraud and Abuse Act to prohibit this conduct. The U.S. provision makes it illegal to:

- knowingly cause the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;
- resulting in a loss of $5000 or more, the injury or risk of medical or public safety, or compromise of certain U.S. systems.

“Damage” is given a special definition to include: any impairment to the integrity or availability of data, a program, a system, or information. This, in effect, makes any transmission of malware designed to damage a computer a

126. Id.
crime, and that includes any impact on data or information, including availability.

The Russian prohibition is broader because it makes the creation of malware a criminal act, something not done by the U.S. statutes, which only penalize the transmission of malware. Thus, a Russian coder researching malware might be in violation for experimentation even when the malware was not transmitted, whereas a U.S. researcher would have to knowingly transmit that code to someone or something. On the other hand, the U.S. statute is broad enough to clearly encompass denial-of-service attacks as damaging transmissions of code. The misuse of malware may be aid in other criminal activity. The distribution of Trojan programs by a virus or fraudulent web site opens a computer to unauthorized access and control, which is a separate violation. Such conduct would be prohibited under both Russian and U.S. law.

D. Procedural Issues

1. Old Crimes and Common Concerns – Procedure and Evidence

A computer may be used to commit a heinous crime like murder. The elements of murder - intent to cause the death of another person, and causing the death of such person or of a third person\textsuperscript{129} - must be met by the facts of the misuse of the computer. The traditional elements of the crime of murder are sufficient. But proving those facts may be the challenge. For example, bludgeoning with a laptop computer would be investigated the same as bludgeoning with a tire iron.\textsuperscript{130} Unauthorized changes in a computer medical record that causes the wrong medication to be fatally given a patient requires a different approach, one that considers what computers do and how their use is different from that of other types of “instrumentalities” of a crime. Specifically, hacking a portable insulin pump via the Bluetooth port to change the dosage to a lethal level would be treated as murder or attempted murder and the investigation would require knowledge of portable electronic systems and how they log system and state changes.\textsuperscript{131}

Critical to the successful investigation of computer crimes is knowledge of the engineering of computer systems, how they work and how the rules of criminal procedure and evidence are applied in this area. While this analysis has focused on new and novel criminal activity using computers and networks, computer and network technologies are used to support many other traditional

\begin{flushleft}
\textsuperscript{130}. In the motion picture “Gattaca” a computer is used as a bludgeon to commit murder. This is not a cybercrime, though a computer was used.
\end{flushleft}
criminal endeavors. They may function much like notebooks, journals, the mail and telephones have done recording and communicating criminal transactions, such as drug or stolen property sales and the coordination of joint crimes and conspiracies. Yet they may offer new twists; instead of using code words to hide the quantity, price and buyer in a drug deal, computer encryption might be used.

<table>
<thead>
<tr>
<th>Contraband</th>
<th>Statute</th>
</tr>
</thead>
<tbody>
<tr>
<td>Child pornography</td>
<td>Possession, receipt 18 USC § 2251</td>
</tr>
<tr>
<td>Obscene materials</td>
<td>Possession, distribution 18 USC § 1460</td>
</tr>
<tr>
<td>Creative content distributed in violation of copyright laws</td>
<td>Copying, distribution 18 USC § 2319</td>
</tr>
<tr>
<td>Trade secret information</td>
<td>Distribution, 18 USC § 1831</td>
</tr>
<tr>
<td>Technology for circumvention of copyright protection technologies</td>
<td>Distribution, Digital Millennium Copyright Act</td>
</tr>
<tr>
<td>Access devices, including passwords</td>
<td>Possession, distribution 18 USC § 1029</td>
</tr>
</tbody>
</table>

A significant challenge in addressing all crimes with computers, including traditional ones, is how the engineering and use of computer systems can be proven in ways admissible in courts. This challenge is one of the law and rules of criminal evidence and criminal procedure. All traditional methods and ways of proof apply to crimes committed with computers. If a person entering the country has a notebook computer with child pornography, a simple border search finding such contraband (see table above) would support a conviction. But if the accused later claims he did not know of the pornography, and that it was placed there without his knowledge by a hacker or spammer, special evidence regarding the operations of computers would be needed to overcome that claim and establish guilt beyond a reasonable doubt.

2. Reliability of Electronic Evidence

Challenges of computer evidence are based on the ease with which electronic information is created, changed, deleted, copied and renamed. A paper document is a fixed rendition of the document. The signature line helps assure that the document was, in fact, signed by a particular person and is associated with that person. But electronic data and documents do not have these features. It is easy to change an electronic document or file so they may

---

132. This type of data is called metadata. See Metadata, TECHTERMS.COM, http://www.techterms.com/definition/metadata (last visited Jun. 17, 2012) ("[Metadata] provides information about a certain item's content. For example, an image may include metadata that describes how large the picture is, the color depth, the image resolution, when the image was created, and other data. A text document's metadata may contain information about how long the document is, who the author is, when the document was written, and a short summary of the document.").
not appear to have been forged absent integrity validation through a message digest or hash value computation on the file. The ease with which electronic information is changed, deleted, copied and renamed is one of the most useful features of word processing and a challenge for forensic purposes. Further, electronic documents and files may be automatically created and changed by the workings of the computers themselves. Simply turning on a computer may make hundreds of file changes. Some of these may be material and raise questions about the reliability of the evidence.

Because of the ease of change and fabrication, a primary hurdle electronic evidence must face is authenticity, that the electronic evidence is what it is claimed to be. This includes the issue of integrity that the evidence is in its original form and has not been materially changed. Authenticity must address baseline admissibility under rules of evidence and the weight as evidence; these reflect the persuasiveness of the evidence, itself an aspect of relevance and weight. Baseline admissibility under U.S. Federal Rules of Evidence requires proof that the item reasonably is what it is claimed to be. The trial judge has great discretion in making that determination. But, even once admitted, the authenticity of electronic evidence may still be challenged as to the degree of reliability that it is what it is claimed to be. The weight of the evidence must still be judged by the finder of fact in a court case, whether judge or jury.

Most computer operating systems keep track of the date and times denoting when the message was modified, accessed or created. A timestamp showing inconsistent times is one way to detect a forgery, but a computer system’s date and time can be momentarily reset and the message saved to reflect that reset time, effectively spoofing the timestamp. However, these issues may not be sufficient to stop a particular email from being used as evidence. The case law regarding the admissibility of documents permits circumstantial authentication to support admissibility. For example, the mention of facts or use of slang or personal terms known only to the people involved in a case may be used to authenticate e-mail sufficient for admission into evidence. But even if admitted, the potential problems outlined can be used to challenge the reliability and weight of the evidence.

Those challenges to weight and responses to those challenges are made both through traditional means (He admitted he sent the e-mail!) and through the developing discipline of computer forensics (The system logs show he sent the e-mail!). Much of the information relating to computer files, databases and electronic evidence is automatically collected by computer systems with no human action. It is not hearsay. Examples are computer network logs of use, cell phone telephone call lists and file MAC times (discussed below). The issue is the reliability of that computer-generated information. If it is normally relied upon for operations, it will probably be found sufficiently authentic for

133. Fed. R. Evid. 901.
admission as evidence unless a challenge is made. And, as with other issues of authenticity, even if admitted the weight of that evidence may still be challenged.

Chain of custody/integrity issues for electronic evidence are particularly important because of the ease of both intentional and unintentional changes to it. A seized handgun will remain in its original form even when examined and test-fired. Turning on a computer to examine it may change certain time and date files and create questions as to who did what. A call to a seized cell phone may delete or change records on it relating to other calls. Special efforts are needed to prevent this from happening and damaging the integrity of the electronic evidence.

The Best Evidence Rule was designed to limit forgery by requiring the “best evidence” of a document be the one used in court, usually the original. This has been relaxed over time. Given that any electronic file must be viewed using a computer, courts permit paper print-outs of electronic files and documents to be submitted as evidence of the computer file and treated as originals under the U.S. Federal Rules of Evidence. The e-mail example discussed above demonstrates possible problems with this. But even if there is some question about the accuracy of the print-out, the solution will not automatically be the exclusion of the paper evidence of the electronic file. Rather, the burden is shifted to the opposing party to investigate and analyze the electronic evidence to show possible forgery; this may go to both admissibility and weight. Such examination may require the use of a specialist in computer forensics.

Within the United States these practices and procedures are encompassed by court rules, case law and statutes governing the administration of justice. The U.S. common law tool of evolving case law has generally been effective in extending precedent to new fact situations involving computing systems. There are some concerns, however, with the scope and scale that may be impacted by these systems. Where a person may now carry their entire personal history in their pocket, a search incident to arrest may produce far more than evidence relating to the detention. Where a search warrant may issue simply because of a credit card number or IP address in a contraband server’s log or data files, the

134. Fed. R. Evid. 1001-08.
136. An IP address - short for Internet Protocol address - is the address of a device attached to an IP network (or TCP/IP network). Every client, server and network device is assigned an IP address, and every packet (unit of data) traversing a network contains a source IP address and a destination IP address. Every IP address that connects to the public Internet is a unique number; however, IP addresses within a local (private) network can be duplicated and are not generally reachable from the outside world. See IP address, PC MAG.COM ENCYCLOPEDIA, http://www.pcmag.com/encyclopedia_term/0,1237,t=IP+address&i=45349,00.asp, (last accessed Jun. 17, 2012).
potential for abuse may be unbounded, at least for those who offend the technically competent.

Addressing concerns in the Russian Federation as to the investigation and regulation of technological systems for the transmission of information via computer facilities involves regulatory and supervisory bodies of executive power. The Russian Federation Service for Technical and Export Control\textsuperscript{137} provides security systems in information and telecommunications infrastructure, that have a significant impact on state security in information systems and telecommunications networks. The Russian Federation Service for Supervision of Communications, Information Technology and Communications monitors and supervises media, including electronic, and mass communications, information technology and communications. It has control and supervision over the conformity of personal data processing requirements of Russian Federation in the field of personal data, as well as the functions for the organization of the radio frequency service.\textsuperscript{138} With the establishment of special executive bodies in the field of electronic and mass communications, information technology and communications in the Russian Federation, the number of offenses have decreased, but that has not solved the problem of combating cybercrime.

Traditional investigative techniques were not effective for detection and investigation of computer crimes. To effectively counter the cybercriminals with good technical equipment and deep knowledge of computer technology, new methods of investigation and crime prevention are necessary. Proper search operations are needed for the collection, analysis and verification of operational and investigative information about the activities of criminals who commit computer crimes. This need for objective monitoring of transmitted information by law enforcement agencies arose with the first use of communications technology for criminal purposes.

Under the Law of the Russian Federation, these techniques of search and monitoring form a comprehensive set of search operations carried out in order to reveal computer crime. They are part of investigation and detection and search operations as stated by the Russian Federation Law “On Operative-Investigative Activity”. These operations include: (1) control of postal, telegraph and other communications; (2) wiretapping; and (3) removing information from technical channels of communication.

Special technical means developed for secretly obtaining information, may be used for monitoring postal, telegraph and other messages. Naturally, to a larger extent, the application of technology refers to “other communications” by


\textsuperscript{138} Положение о Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций: Постановление Правительства РФ от 16 марта 2009 г. № 228, Regulations on Federal Service on Supervision in the sphere of communication, information technologies and mass communication.
which under Part 2 of Article 8 and Part 1 of Article 9 of the Federal Law “On the Operative Investigative Activity” it means messages sent over the telecommunications networks and postal services. In its turn, in Article 2 of the Federal Law “On Communication,” the notion of an electrical connection is interpreted as follows: “Any transmission or reception of signs, signals, writing, images, sounds by wire, radio, optical or other electromagnetic systems; telecommunications network - technological systems that provide one or several types of transmissions: telephone, telegraph, facsimile, data and other documentary communications, including the exchange of information between computers, television, sound and other types of radio and wire broadcasting.”

This provision of the Law “On the Operative Investigative Activity” permits the use of technical means to monitor all kinds of messages transmitted by wire and radio channels, including the messages transmitted by cellular systems (SMS, E-mail, WAP) and paging. The division of information on other messages, phone calls and the information transmitted through technical channels of communication, stated in the Law “On the Operative Investigative Activity” is out of date and does not comply with modern realities in the field of information transmission systems. Specifically, at present, it is not appropriate to refer to a clear division of information on modes of transmission. For example, cellular communication allows one to send and receive emails, SMS-message, fax, and computer-assisted telephone calls (IP-telephony) and faxes, while the signals carrying the information can be transferred in stages by radio, wire and fiber-optical communication channels.

The above can also be extended to the operative investigative measures, called “wiretapping” and “of information from technical channels of communication,” because currently it is not necessary to use a telephone to make telephone calls. And, although the concept of “technical links,” which occurs in the Law “On the Operative Investigative Activity,” can be found in 40 Acts of Legislation of the Russian Federation; it has no clear definition, and therefore it seems difficult to determine its legal meaning.

Removing information from technical communication channels described as operational search activities is activity for the purpose of obtaining secret information about the behavior and actions of individuals suspected of...

committing crimes by controlling special technical means of electromagnetic and other fields, arising from the transfer of information on various telecommunications networks connected to computer networks, databases, information retrieval systems, telecommunications systems that collect, process, accumulate, store, retrieve and disseminate information. Since the introduction of technical communication, this activity was strictly clandestine; it was a state secret and only regulated by internal regulations. Similarly, within law enforcement agencies, the use of operational and technical means associated with the removal of information from communication channels was strictly secretive. Strict regime rules for these activities were implemented. The results of the removal of information from technical channels of communication, as a rule, could not be used as evidence which had a negative influence on the investigation of criminal cases.

Large-scale dissemination of information and telecommunication networks required systemic responses to crime in this area. Therefore, the System Operational-Search Measures ("SOSM") were developed in the 1990s. 142 SOSM is an automated information system for special purposes connected to the switching equipment and telecommunication operators and is designed to provide search operations conducted within a public telecommunication channel. The first stage of development involved the placement of SOSM on public phone lines. To formalize this regulatory step, a Directive Letter of the Ministry of Communications of the Russian Federation was issued. 143

The second phase of SOSM was implemented in 1998. It established appropriate specifications for SOSM at stationary switching equipment of telecommunication systems of electro-connections, which provided access to the computer network/"Internet". Due to imperfections and regulations adopted by the Ministry of Communications, this phase was challenging. In particular, operators were required, at their own cost, to connect terminal equipment to SOSM technological systems. This requirement did not comply with current legislation and caused significant righteous indignation and reluctance to carry unforeseen material costs. The situation was exacerbated as simultaneously the State Technical Commission under the President of the Russian Federation brought its fair, but strict requirements for providers - the need for training and certification of information security managers, again, at the expense of providers. 144 Most of the providers eventually complied and connected to


144. Id.
SOSM, akin to the compliance by U.S. telecommunication operators with the Communications Assistance with Law Enforcement Act (CALEA). In 2000, the third stage began. It was marked by the publication of the “Order of the Ministry for Communications and Information.” The fourth stage was put into practice on January 1, 2006, with the ratification of the Russian Federation Government Resolution of August 27, 2005 № 538 entitled, “On Approval of Rules of Interaction of Operators with the State Authorities Carrying out Operational Search activities.” The rules defined the scope of interaction of operators with the state authorities – the Federal Security Service of the Russian Federation (“FSB”) and the Ministry of Internal Affairs of the Russian Federation (“MVD”), when performing operational-search activities with the use of SOSM in accordance with Russian Federation Law “On Operative-Investigative Activities.” Service providers must file an application not later than 60 days from the date of receipt of the license to provide telecommunication services. Then the head of the local FSB of Russia in response to an application determines the relevant department of the FSB of Russia to interact with the service provider.

In accordance with Clause 12 of these rules, every telecom operator (Provider of Internet Services) is required to promptly update information contained in databases of subscribers (customers) and provide them with telecommunications services. This information should be stored in a service provider for three years and made available to agencies of the FSB or MVD.

through round-the-clock remote access to databases. These databases must contain the following information about the subscriber service provider: (1) surname, name, address and details of the main identification document presented by personal presentation of the subscriber of the document - for subscriber-citizen; (2) name (company name) of a legal entity, its location, as well as a list of people who use the terminal equipment of a legal entity, certified by an authorized representative of the legal entity, which indicated their surnames, first names, middle initial, and place of residence and details of the main document of identity - the subscriber - legal entity; and (3) the information database on payments for services rendered communication, including connections, traffic charges and subscribers.\textsuperscript{151}

There are requirements for telecommunication networks, members of the public communications network and communications network to carry out operative-search activities.\textsuperscript{152} Additionally, there are requirements for equipment terminal transit nodes of networks of mobile radio communications using circuit switching technology, and/or the packet of information included in the public communication network, and dedicated networks of mobile radio communications, including software that provides fulfillment of the established operations for these search activities.\textsuperscript{153}

The technical equipment for operative – search activities on terminal transit nodes of mobile telecommunication networks provides that:


(1) access to the information, transmitted in the connection and (or) in the message of the telecommunication of the subscribers and access to the information about the location of subscribers that are to be checked; (2) the possibility of introducing the data list and recording of the data including subscribers’ numbers and (or) descriptors (accounts) with the control parameters. The parameters are preset by the command transmitted from the point of control of the law enforcement agency that is performing the operational-search activities.¹⁵⁴

The most important requirement for functions of the technical equipment for operative – search activities is the control of the location of the objects:

(a) while establishing the connection between the subscribers under control; (b) for updating the data of the location of objects under control; (c) at the time of switching on, switching off, registering or deregistering of the equipment of objects under control; (d) at the time of registration of the equipment of the objects under control while roaming in a visiting network, indicating the identifier VLR ID; (e) while removing and installing the SIM-card of GSM or similar cards used in other MTS; (f) at the time of sending or receiving faxes, SMS, EMS, USSD, video calls by the objects under control.¹⁵⁵

The information about the location of the object under control, based on the standard and availability of such information, contains one or more of the following types of location data control objects: (1) global cell ID; (2) The zone ID routing; (3) positioning of GSM; (4) positioning of the UMTS; (5) The zone ID user. These legislative measures facilitate the identification of perpetrators of computer crimes. Thus, the use of operational search activities in the investigation of computer crimes is important, but the results must be presented to the investigator in a timely manner and in accordance with the law.

The Russian Federation Law “On Operational-Investigative Activities” (parts one and two of Article 11) establishes that the outcome of operative-search activity can be used for the preparation and implementation of investigative and judicial actions and to conduct search operations. They can serve as both an excuse and reason for criminal proceedings, submitted to the

¹⁵⁵. Id.
inquiry body, investigator or the court handling the criminal case, and also can be used as proof in criminal cases in accordance with the provisions of the Criminal Procedure Code of the Russian Federation. Accordingly, the Code of Criminal Procedure prohibits the use of results of operative and search activities of evidence in trial, if they do not meet the requirements of the Criminal Procedural legislation.

Of particular importance in the formation of information from technical channels of communication are the “Instructions on how to present the results of operative investigation to the inquiry body, investigator, prosecutor or the court.” This Instruction integrates the two branches of law: criminal-procedural and operational search. The Constitutional Court of the Russian Federation has repeatedly affirmed the legality of investigative activities. In one case the Constitutional Court of the Russian Federation noted that use of information systems, video, audio, film and photography, as well as other technical and other means, during search operations, without harm to human health and life and without harm to the environment, is provided for in Part 3 of Article 6 of the RF Law “On Operative-Investigation Activity.” This section directs the conduct and outcome of these search processes. The use of technical means, including means of audio, is part of the general order of the search operations and recognizes an obligation for separate search operations and restricting the constitutional rights of an individual and citizen.

Analogues of the Russian SOSM exist throughout the world. Eligibility and use requirements for such systems are distinct for each nation. The difference is

159. Инструкция о порядке представления результатов оперативно-розыскной деятельности дознавателю, органу дознания, следователю, прокурору или в суд: Приказ МВД России, ФСБ России, ФСО России, ФТС России, СВР России, ФСИН России, ФСКН России, Минобороны России от 17.04.2007 N 368/185/164/32/184/97/147 // Рос. газ. 2007. 16 мая. Instructions on procedure of reporting the results of operative investigation to investigator, inquiry body, investigator, prosecutor or the court: Order of the Russian Interior Ministry, the FSB, Russia.
161. Id.
characterized not only by the requirements of application systems, but also by the manner of constructing of the general model of interaction between the system components. A key factor may be that such systems may have few, if any, restrictions as they relate to transnational and international data transfers but significant restrictions for domestic data surveillance.

For example, the “Echelon” systems (“Echelon”) operate across five countries: U.S., Canada, Australia, New Zealand, Great Britain, signatories to the United Kingdom under a United States of America Agreement. The agreement addresses national systems of operational search activities of the nations through communications systems which collect signal intelligence from other nations, although historically the Agreement focused on the then Soviet Union. Those systems and related agencies are:

1. In the United States - National Security Agency (National Security Agency - NSA), the official site which is located on a computer on the Internet at http://www.nsa.gov/;
2. In Canada - the Committee of safety and control of intelligent information (Security Intelligence Review Committee - SIRC), whose official website is located at http://www.sirc-csars.gc.ca/;
3. In Australia - Signal Security Administration (Defense Signals Directorate - DSD), which is represented on the site http://www.dsd.gov.au/;
4. New Zealand - Government Communications Security Bureau (Government Communications Security Bureau - GCSB), the site which is located at http://www.gesb.govt.nz/; and
5. In the UK - Head of Government Communications (Government Communications Headquarters - GCHQ), which has an official website for http://www.gchq.gov.uk/.

Domestic electronic surveillance in the United States is subject to a variety of statutes that require various levels of detail that criminal activity is underway, depending on the nature of the electronic communications. Domestic electronic surveillance related to national security matters requires a lesser showing that a surveillance subject is a foreign entity or an agent of one; this is subject to special oversight, including that of the Foreign Intelligence Surveillance Court.

The Constitution of the Russian Federation contains the guarantees of freedom of expression and information exchange (the right to seek, receive,
transmit, produce and distribute information in any legal way), as well as the 
prohibition of censorship. The basic law of Russia limits human rights and 
freedoms in the interests of others, society, and the State. Additionally, 
these rights guaranteed by the Constitution of the Russian Federation “may be 
limited by U.S. law only to the extent that it is necessary to protect the 
constitutional system, morality, health, rights and lawful interests of other 
persons, national defense and national security.”

Special technical activities are carried out and documented in accordance 
with the requirements of the Law “On Operational-Investigative Activities,” 
which regulates operation search activities. Because of the potential for these 
special technical measures to affect the constitutional rights and freedoms of 
citizens, Russian Law “On Operational-Investigative Activities” requires a 
judicial decision and a resolution from the body conducting the investigation as a 
prerequisite in conducting search operations (including the use of technical 
means, which include radio transmitters), which limit the constitutional human 
and civil rights (secrecy of correspondence, telephone conversations, postal, 
telegraph and other messages sent by telecommunications networks and postal 
services, as well as the right to inviolability of the home).

Given current trends in the integration of criminal procedure and search, 
there is an urgent need to include the new investigation activities aimed at 
obtaining evidence in information and telecommunications networks into 
Criminal Procedural Code of the Russian Federation. The present Criminal 
Procedure Code of the Russian Federation provides for a new investigative 
action - getting information about the connections between users and (or) 
subscriber units (Art. 186.1 CCP) introduced in 2010 that allows the 
investigator to obtain such information by judicial decision. A copy of the court 
order is sent to the appropriate investigator by the communications services 
organization, whose director is obliged to provide such information as recorded 
on any physical carrier. The information is provided under seal with a cover

166. See Конституция Российской Федерации [Конст. РФ] [Constitution] art. 29 (Russ.).
167. See Конституция Российской Федерации [Конст. РФ] [Constitution] art. 17, part 3 (Russ.).
168. See Конституция Российской Федерации [Конст. РФ] [Constitution] art. 29, part 2 (Russ.).
169. See Конституция Российской Федерации [Конст. РФ] [Constitution] art. 5, part 1 (Russ.); accord Конституция Российской Федерации [Конст. РФ] [Constitution] art. 56, part 1 (Russ.).
170. See Конституция Российской Федерации [Конст. РФ] [Constitution] art. 55, part 3 (Russ.).
letter stating the period for which it is provided and the number of subscribers
and (or) user devices. While this law provides coverage for subscriber
information, and also the seizure and investigation of postal and telegraph
communications, the current definition in the law “other post and telegraph
communications” is not quite clear as to whether or not this included email
communications. Additionally, the law does not mention e-mail messages as
types of mail and the procedural consequences related to the seizure of postal
and telegraph involving actions on the part of operators in the seizure of emails
is inapplicable. Certainly, there is a need to specify the procedure for seizure of
an e-mail network in the investigation of computer crimes

3. Computer and Digital Forensics and Investigations

Computer and Digital Forensics professionals investigate, collect, analyze
and report on electronic evidence. This discipline relies on the special features
of computer and network information that create a wealth of evidence; those
features include: (1) persistence of electronic information across multiple
locations due to the lack of a true “delete” function, (2) automatic copying of
electronic information to multiple locations in and outside of the creating
computer, and (3) creation of metadata, or “data about data” for each electronic
file created.

Persistence of Data - Deleting an electronic document does not eliminate the
document. Many operating systems have virtual “trash cans” where “deleted”
files are listed should the file later be needed. More fundamentally computer
operating systems do not waste resources to actually erase data for a deleted file.
Computers store information electronically on a hard disk or other media using
the card catalogue and book shelf model of a library. The information is stored
someplace (sometimes in many places) on the media (the book shelf). When a
computer file is “deleted” the computer simply notes the deletion in the file
index, which now makes the old locations available to write new information.
But the old information continues to exist on the media until that happens or a
special cyber-shredding program is used to destroy it. A computer file index (the
card catalogue) lists where the information can be found, and also tells the
computer not to write over that file and scramble the data. To use a file the
computer looks up the locations from the file index and reassembles the file.
Because of this, computers are excellent sources of electronic evidence for law
enforcement due to the difficulty of actually destroying electronic information.
It also indicates the problems of privacy with computers where proper document
cleansing procedures are not followed.

Multiplicity of Copies - Computer operating systems may make multiple
copies of all or part of an electronic document and scatter it about the computer
and network, simply as a matter of how they are designed. A sent e-mail creates
a copy in the sender’s “sent mail” file, one in the recipient’s mail file and copies
in computers along its route to the recipient, some of which might store the copy
in their back-up files. A web browser does more than retrieve a copy of web page for viewing; it tracks a user’s web excursions. It stores “cookie” files and copies of web pages and the addresses of the recent web pages visited. It also sends out information on the user’s computer, including Internet Protocol addressing information, to remote computers when requesting a web page; this information may be tracked by that remote computer.

To handle large files, computers may momentarily store works in progress in “swap” or “page” files. Once the work is done the information is ignored, but as with deleted files it remains until written over by other information. As page or swap files may be huge, lots of information may remain even if the original file is deleted and cyber-shredded.

**Meta-data** - All but the most primitive electronic documents and files contain “hidden” information not seen in the paper printout or rendered in the usual on-screen display. Some of that hidden information controls features of electronic documents beyond the text itself. Other kinds of information assist in document and file management and collaboration, locally or over a wide network.

Such “data about data,” or “metadata,” permeates the electronic world, whether added to a document manually by an author or automatically by a computer. That hidden metadata is relevant as computer evidence because it reveals when or how a document was made and potentially the provenance and thought processes behind that document. A MAC time showing a recent e-mail file modification time different from the creation time may indicate a forgery. MAC times showing various recent access times of child pornography images, well after the creation times, can be evidence of knowing and recent possession and use. Conversely, a group of images with nearly identical creation times and access times equal to creation times may indicate an automated function, such as a Trojan program or third party use such that the owner did not know of or use the images. Network activities have their own types of meta-data of information transactions. Network logs track all traffic through their systems and collect address, day and time information from that information. This information can be collected and correlated as evidence of if and when certain network activity, including over the Internet, occurred.

**Computer Forensic Examination and Tools** – The acquisition and explanation of digital evidence may require multiple skills. Some of this electronic evidence can be found by the simple use of a computer, such as a cell phone or e-mail program. Specialized knowledge is not needed. Other evidence may require special tools to find. And still other evidence, such as explaining MAC times, might require the knowledge of a special qualified expert.

**Lay Witnesses** - Word processing, spreadsheet, e-mail or web files can all be examined using the applications programs normally used for such activity. If only the possession of the information they represent is the issue, then examination and presentation as evidence is sufficient. But that examination
itself changes files, especially the meta-data, and may compromise the integrity of the evidence.

This issue related to the examination itself changing computer files creates a **chain of custody/integrity** issue. This problem can be addressed by tools called **write-blockers** and **bit-copy/mirror copies**. The write-blocker prevents a computer from changing files when an examination begins and preserves the integrity of the information. The bit-copy/mirror copy is an exact, physical copy of the entire item being examined, like a hard drive. The examination is done on the mirror copy without writing any changes to it; this preserves the original evidence and protects it from claims that the evidence was changed. The deleted files may be “undeleted” and “File Carving” programs can reassemble deleted files where part of the file has already been overwritten and destroyed.

Another problem with computer evidence is the amount of information on modern computers. It is so great that a computer may take hundreds of hours to examine. Forensic programs assist with this by automatically indexing all the files on a computer by file name, location, file type, file extension, content text and other properties. These forensic programs use filtering features to assist with the examination of the results by marking known programs that are standard on computers, such as operating system files. They then search for known illegal programs, like previously seized images of child pornography, and flag those programs. These filters greatly reduce the time needed for an accurate examination of the electronic evidence, although there is a growing need for computational systems to take on more of this analysis.

**Expert Witness** – At some point, there may need to be specialized knowledge of computer operations that is outside of normal experience with computers. If that specialized knowledge meets tests of reliability, it can be used as additional evidence to explain what a particular bit of electronic evidence means. Those tests require proof of 1) adequate specialized knowledge, 2) applied to sufficient data, 3) using reliable methods, 4) applied properly. For example, in one case the prosecution sought to introduce evidence regarding when certain files had been accessed/created/read based on registry information without qualifying the evidence as expert opinion. The United States Court of Appeals for the Sixth Circuit recently noted that:

> Software programs such as Microsoft Word and Outlook may be as commonly used as home medical thermometers, but the forensic tests [here] are more akin to specialized medical tests run by physicians. …The average layperson today may be able

---

173. Fed. R. Evidence 702 ("If scientific, technical, or other specialized knowledge will assist the trier of fact to understand the evidence or to determine a fact in issue, a witness qualified as an expert by knowledge, skill, experience, training, or education, may testify thereto in the form of an opinion or otherwise, if (1) the testimony is based upon sufficient facts or data, (2) the testimony is the product of reliable principles and methods, and (3) the witness has applied the principles and methods reliably to the facts of the case.").
to interpret the outputs of popular software programs as easily as he or she interprets everyday vernacular, but the interpretation [the government’s examiner] needed to apply to make sense of the software reports is more similar to the specialized knowledge police officers use to interpret slang and code words used by drug dealers.  

The court found that this information could only be interpreted by an expert if that interpretation was found to be sufficiently reliable. These issues of reliability and the need for particular kinds of special services to properly analyze computer evidence will continue to develop and change just as these systems develop and change.

In both Russia and the U.S., training of law enforcement officials in this sphere is critical. Special anti-computer crime training programs for investigators should be used. In the United States, there has been extensive training of law enforcement through programs such as the Internet Crimes Against Children (ICAC) initiative, which offers training on electronic search and seizure applicable to both child exploitation (child pornography, child internet seduction) cases and other cases involving electronic evidence. Advanced investigations involving network forensics, often key to unauthorized access cases, benefit from investigators with advanced training. The Russian Federation officials that work in this sphere should, ideally, have a degree in law and degree in engineering. Such specialists should be able to deal with the following issues: investigation of the cases of unauthorized access to computer information and assistance to an investigator in describing computer equipment and other equipment in the protocol of the interactive actions, doing express-analysis of computer information; tracing information; preventing information from destruction or modifying; retrieval of information etc.

Computer specialists should also have knowledge about the components of a computer, its software and hardware and its operating functions. In the case of remote illegal access, the specialists should be able to deal with software and programming and computation as well as networks and communication devices. The progression of events that take place at a crime scene are extremely important. The process should unfold as described below for maximum efficacy.

(1) Before arrival at the crime scene

Important organizational issues must be considered before arrival at the scene of crime. First of all, computer specialists need to be provided with some specific equipment to do digital examination (a special cable; special software,  


which allows copying and rapid analysis of information on the site; hard drives of a larger volume or equal to that of the computer hard drive under examination; various carriers to transfer onto and store the copied information (e.g., an additional portable hard drive). Secondly, witnesses should be provided. These people could be specialists in computer science. Thirdly, investigators and computer specialists should give special instructions to all members of an investigative team. In particular, some special attention should be focused on their careful behavior concerning computer equipment at the scene of crime. Also, the computer specialist’s work should be provided with favorable conditions. Finally, investigators should consult computer specialists on the most complicated technical issues.

(2) Arrival at the crime scene

Immediately upon arrival at the scene of crime, investigators observe the scene and the availability of computers and other equipment. It is desirable to make an overview and apply photo-video recording. It is necessary to exclude any possibility of unauthorized persons to use the equipment. These people should not use the telephone as well. If there’s an urgent call, it should be permitted by the investigator only.

(3) Investigation of the crime scene

Computer safety specialists check on whether the computers are connected with the local network. Provided that a local network is running, it is necessary to examine the server that contains most portion of information. If the computer specialist finds out that the program has been deleting or decoding the information, these programs are closed and this computer should be carefully examined. Additionally, every other object is thoroughly checked. While examining it is necessary to establish whether the information can be used as evidence for some further investigation.

At this stage, the general configuration of the computer system is determined (the version of software, processor type, memory volume, user information etc.). For this in the sub manual “properties” the folder “system” is chosen and the content is reported in the protocol.

The current condition of the computer information is analyzed and reported: the findings, destruction of information, copying, blocking of information, damaged information and modified information, breaking computers, computer systems and network and the way the crime was committed.

If it is established that “direct” access to the computer took place, it is necessary to search for fingerprints and micro particles on the keyboard, the furniture, the computer, the monitor, the computer, the printer and other devices. Moreover, the investigator should check on several documents: the documents related to the crime committed (accounts of paroles and logins); the documents reporting on an attempt to transfer the information onto a paper; the technical documentation on the computer, software or other device, the documents which contain the schedule and the order of work with the computer equipment.
If the investigation of the crime scene takes several days, the place is locked and sealed and the electrical supply is cut off. If the paroles and logins are not determined, the computer and the processor are confiscated. Magnetic media should be transferred in the space and stored in a specially sealed and shielded container. The remaining parts of the computer—keyboard, the monitor and the mouse should be sealed.  

The configuration of the computer should be described in detail including inventory numbers, models and serial numbers of each device and other information provided on the labels by the producer. All the information from the hardware should be copied as well as printed out or hand written. All pages should be signed by the specialist, the investigator, the witnesses and, where appropriate, the representative of the organization where the search was conducted. This information should be attached to the report.  

The program being used at the time of search should be described in the report. Computer specialists examine and describe the following: the icons on the computer screen and all the functioning peripheral devices and their data and the data of the detected program and the manipulations with the computer (including the pressing on the keyboard), produced during the investigation and the results. Removing of the computer equipment is conducted when it is switched off.

To determine whether illegal access to computer information took place, some investigative activities are carried out. There are also a number of best practices to consider upon leaving the crime scene and continuing other investigative activities. These practices are outlined below.

The victims are interviewed regarding how the victims’ data were used; the amount damage; their provider; the user’s login information. In most cases, the witnesses in this category of crime are persons with higher education with perfect knowledge of special terminology, which is not often clear for the investigator. Due to this, the investigator should obtain detailed evidence of the interrogated by a number of clarifying questions, revealing this or that term and/or a definition, used by the interrogated. A computer safety specialist can be involved into the interrogation procedure as well. In the course of interrogation of the witnesses it is necessary to ascertain a number of issues relating to system operations.  


178. Did anyone show any interest to the computer information, software, computer equipment of this enterprise? Did any strangers appear on the premises where computer equipment is located? Were there any cases of the staff working with the information which beyond their competence? Have there been any recent network, electronic, computer information protection failures reported? How often are the software programs checked for viruses, and what are the results of the recent check-ups? How often is the software upgraded? How, where and by whom it is purchased? How
After that, a provider is asked to give information on the subscriber for a given period of time, with the indication of the date, the beginning, the duration of work and the withdrawing money, access point, IP address and MAC address. Investigation of the crimes that are committed with the use of remote access to computer information should be conducted in cooperation with the ISP (service providers). In accordance with Article 2 of the Federal Law “On Communication”, a service provider is a legal entity or individual entrepreneur who provides communication services to subscribers on the basis of a license.\

In an investigation into computer networks, information signs can be used. These represent information about the subscriber, the passage, and communications that are stored in the provider’s log files. The information, contained in the log-files can be needed for establishing circumstances of the illegal access (e.g. identification of a subscriber in the network). For successful evidence collection, the investigator must timely store the data he or she gathers. In connection with the high latency of such crimes, the investigation often commences a long time after the crime was committed. This is why it is necessary for legislators to set standards for data storage, requirements related to the type and volume of the computer information to be stored, and the order of its documentation if the case is transferred to law enforcement bodies. Not all data is stored in required volumes and much of the information may be deleted if not quickly retrieved.

In the “Guidance for interaction of service providers with governmental officials that do investigation work,” an operator is obligated to upgrade information, including services provided, in the subscriber database. The information is to be stored within three years. The following information should be provided: name, patronymic, surname, place of living, the details of the ID

is the repair and upgrading carried out? What is the order of working with the information, how is it obtained, processed, and transferred through the connection channels? How is access to the Internet carried, who has the right to work in the net what are their credentials? How is protection carried out? Did other cases of illegal access to computer information take places before, if yes, how often? Could the consequences be the results of careless action of a person or errors in the work of computer or software failures? What are the specifics of modification of information? Who is the owner of the information that was wrongfully accessed? All these questions should be clarified with the computer operators, programmers, computer safety specialists and the managers of the enterprise.

document; the data about the accounts and payments for the services, including connections, traffic. At the same time the amount of the data about the connections to be reported is not established in law (IP—statistics, MAC-statistics etc.). The detailed statistics, including the data about visiting certain sites and which is of a special interest to the investigation is to be stored for approximately three months.

Investigations of illegal access to computer information have presented challenges to the ability to obtain evidence. Within the Russian Federation, service providers have refused to provide the data without a court order, based on Part 3 Art.63 of the Federal Law “On communication.” The Constitutional Court of the RF expressed the same position in the Court Decision of 02/10/2003 N 345-O, which explained that private telephone conversations cannot be disclosed without a court order. This includes the technical data about the input and output signals of the communication subscribers.

The Russian Federation Government Resolution N 538, Article 12 provides that enforcement agencies with 24 hour remote access to databases of subscribers. E.K. Volchinskaya believes that this article inhibits operators’ ability to follow a court decision to provide information about the connections. It only means internal control.

A.E. Fedyunin asserts that all types of removal and audit information restrict the rights of citizens, specifically those rights indicated in Part. 2 Art. 23 of the RF Constitution, and that the removal and audit information can be enforceable only on the grounds of the court decision. Conversely, Y.N. Sokolov thinks the court order providing for data receipt should be kept and regulated at the level of the current legislation.
In July 2010, legislators introduced a specific investigative action, stated in Article 186.1 of the Code of Criminal Procedure.\textsuperscript{187} The action involves gathering information about the connections among subscribers and (or) subscriber units.\textsuperscript{188} Gathering information is defined as collecting the data on time, duration, connection between the subscribers or subscriber units, ID addresses and the locations of the access.\textsuperscript{189} In practice, the information which is being obtained is related to the Internet-session of the subscriber.\textsuperscript{190} The information about the ID addresses is provided upon request.\textsuperscript{191}

Service providers can be interviewed about the above mentioned issues. They are required to provide investigators with copies of all constituent documents and licenses.\textsuperscript{192} In the course of investigation, the interrogation of the suspect is of crucial importance. It is necessary to determine how network access was obtained and to determine the computer skills of the suspect and characteristics of the computer being used.

During the preparatory work, prior to a search, it is important for the investigator to determine the following: what equipment is situated on the premises; the source of energy, the local network and access to the Internet used by application software; availability of data security, encryption, and other forms of security. A specialist in computer systems should be used to prepare the appropriate computer equipment to be used for reading and storing information that has been extracted. Information on the identity and background of the computer owner, their professional computer skills, and the best time and date for the search to ensure confidentiality of the search (the most successful are the early morning hours - from 6:00 AM to 8:00 AM), as well as to produce the best information available from the computer.

Once the preliminary information has been collected, the investigator, based on a court order, has the right to conduct a physical search. The physical place to be searched is usually a residence or business. Among business organizations, those engaged in the sale of computer hardware and software, computer centers, Internet cafes, computer education classes, computer clubs are all significant sources of evidence. These searches however, are complicated by the large

\begin{thebibliography}{99}
\bibitem{187} UGOLOVNO-PROTSESSUAL'NYI KODEKS ROSSII FEDERATSII [UPK RF] [Criminal Procedural Code] art. 186.1 (Russ.).
\bibitem{188} Id.
\bibitem{189} Id.
\bibitem{190} Id.
\bibitem{191} Id.
\bibitem{192} Medvedev V.N. The objective necessity of removing information from technical channels of communication to combat crime.
\end{thebibliography}
amount of computer technology and equipment, as well as the open nature of the access sometimes provided.

Entry to the physical facility for the conduct of a search should be without prior notification and swift to minimize the occurrence of evidence within the computers. In some cases if appropriate, the computers should be disconnected before the search takes place. One should remember that such action can lead to disabling of the entire device (cause damage to it). Information on such computers shall be deleted as well.

Immediately following entry to the search location, all personnel not participating in the search should be removed. The physical location of the computers should be identified and inventoried. Those computers which have active and open programs running at the time of the search should immediately be checked by a computer specialist; also, special measures should be taken to stop the program and check the contents of the computer storage mechanisms.

The detailed phase of the search is the most time-consuming. Investigative actions should be taken to identify hidden information. Information may be disguised in many locations on a computer and in many forms. One aspect of the evidence can be digital archives stored at the computer. Also, laser discs, external hard drives, or other carriers can be used for storing information, and should be taken as evidence.

If there a network located in the facility being searched, location of the servers must be identified. Special attention should be focused on unconnected sockets, cables, free sockets, because this may be an indication of computers that have been removed and hidden in other locations. Computer specialists follow special procedure of taking digital evidence. They make a copy of the digital evidence and transfer it on other carriers (laser discs, hard drives etc). These carriers should be packed in plastic boxes then sealed.

Since it is not always possible to process large quantities of information directly, it is best to remove the information, store it on a separate system and then engage in the data identification and extraction procedures. In many cases it is simply a matter of removing the hard disk from the computer or the system unit. It should be noted that it is advisable not to remove all the equipment in order to prevent claims from the owners. Specifically, the removal of printers is not advisable as the identification of the information on the remaining prints is impossible. The devices with the copied information should be packed and sealed. If this is not possible, it is advisable to remove the entire computer.

Most computers do not have serial or manufacturer numbers for the entire machine, but they can be found on the components of computer (hard disk, drive, motherboard, CPU, power supply, video and sound cards). For an exact identification all the built-in cards should be listed in the search protocol. When removing the hard disk the details such as the manufacturer, type, country, technical characteristics, and serial or manufacturer numbers should be noted in the protocol. A portable computer should be removed as a whole. At the final
stage of the search a protocol (search methodology, step-by-step) is created as well as inventory, plans and schematics of the searched premises.

The role of digital and computer forensics is common to both the Russian and U.S. systems, though there may be some procedural differences in the application of those analytics. In Russia, the investigation of illegal access to computer information includes various types of expertise, including forensic (trasologiya, fingerprinting, etc.) and computer-technical expertise. E.R. Rossinskaya and A. I. Usov consider computer-technical expertise as a separate kind of forensic expertise and is a specialized engineering and technology expertise. They classify this technical expertise into the following categories: computer hardware expertise, computer software expertise, computer forensic information expertise and, computer-networking expertise.

Hardware computer expertise is the study and understanding of technical computer systems. The issues addressed within this type of expertise include: What are the technical parameters and characteristics of the computer? What is its functional purpose? Is the hardware part of a computing system? What was the configuration data of the hardware? What is the actual state (faulty, defective) of the device? Are there any deviations from normal parameters? Computer software expertise provides answers to the following: Were modifications made to its security protection system? In what way was it modified (deliberately, virus, errors, etc.)? What is the chronology of the modifications in the software? What are the consequences of the further exploitation of the software?

Forensic information presents skills to solve diagnostic and identification that necessarily arise in identifying and extracting the digital evidence. This may include: How was the computer information formatted and how is it dated? What were the characteristics of physical placement of the data on the computer? What properties, characteristics and parameters (volumes, dates of creation-modification, etc.) of the data are maintained on the computer? What type of data access is provided (free, limited or other)? What capabilities exist within the computer to overcome internal and external protective devices and operations? What is the content of the protected data? What is the actual state of the data identified and does it correspond to comparable data on a similar computer containing the same or similar information? How were the data operations (blocking, modification, copying, removing) on the computer performed?

Forensic computer-network expertise is used to identify technical network information (for example, investigation of the facts and the circumstances, related to use of the network and related telecommunication technologies). It


can provide information on the following: Are there any indications this computer device was communicating with the Internet? Are there readily available means to connect to the Internet? What are the properties of these available means of connection? What Internet addresses exist where access occurred?

4. Computational Forensics

The investigation of cyber and computer crime offers new opportunities and challenges in various forms of computer forensics. The conclusions may be used as evidence and consequently, are open to challenge in the following ways:

1. evaluation of the system used in computer forensics against the general legal framework for evidence,
2. measurement of computationally-based conclusions against one or more tests for reliability and
3. the weight of their conclusions in a judicial determination. \[195\]

Computational Forensics (CF) has been described as

... an emerging interdisciplinary research domain. It is understood as the hypothesis driven investigation of a specific forensic problem using computers, with the primary goal of discovery and advancement of forensic knowledge. CF works towards (1) in depth understanding of a forensic discipline, (2) evaluation of a particular scientific method basis and (3) systematic approach to forensic sciences by applying techniques of computer science, applied mathematics and statistics. (Franke and Srihari 2007)

Yet, as with the introduction of all expert systems for forensic evidence, the key issue is the reliability of the conclusions revealed amidst the smoke and mist of technology.

Computational forensics is evolving within both U.S. and world law. Its promise is that informatics systems can do analysis on the terabyte scale that now begins to elude human investigators using simple rule-based filtering to find evidence. The danger of computational forensics is in establishing its reliability, particularly in the use of statistical methods, sufficient to meet the needs of justice.

5. Cyberterrorism

Dorothy Denning described cyberterrorism as “the convergence of terrorism and cyberspace.” \[196\] It is generally understood as unlawful attacks and threats of

---

195. Legal Issues in Research and Practice With Computational Forensics.
attack against computers, networks, and the information stored therein when
done to intimidate or coerce a government or its people in furtherance of
political or social objectives. Further, to qualify as cyberterrorism, an attack
should result in violence against persons or property, or at least cause so much
harm that it would generate fear. The examples of such attacks are those that
cause death or bodily injury, explosions, plane crashes, water contamination or
severe economic loss. Serious attacks against critical infrastructures could be
acts of cyberterrorism, depending on their consequences. Attacks that disrupt
nonessential services or that are mainly a costly nuisance would not be
considered as cyber terrorist attacks.

Director of the Center for Protection of National Infrastructure of the US
FBI, Ronald Dick, in a report published on the website of the U.S. Bureau of
Investigation, said that “... in the world a new form of terrorism - cyberterrorism
has been formed”, which uses computer and communications network for the
destruction of parts of the national infrastructure to achieve their goals. Every
day we are faced with computer attacks in government agencies. The Achilles
heel of the modern world is a growing dependence on computer systems and
information technology.”197 The introduction of modern information technology
has led to new types of crimes, such as computer crime and computer terrorism -
illegal interference in the network services, electronic systems and computer
networks, theft, misappropriation, extortion of computer information, the impact
of using computer technology on people and agencies of public authority.

In Russia, according to the Russian Institute of Contemporary Development,
the number of Internet users in 2011 was about sixty-six percent of the total
population (more than eighty-five million people). 198 In such circumstances,
computer technology and the Internet become a necessary expanded social
infrastructure. In the Okinawa Charter on Global Information Society, it is noted
that “… information technology, telecommunications is one of the most
important factors influencing the formation of a society of XXI century. Its
revolutionary impact affects the way people live, work, and get education as well
as the way government interact with the civil society. Information and
communication technologies are rapidly becoming an important stimulus for the
development of the international community.”199

Dissemination, information and technological capabilities of IT systems led
to the specifics of computer crime in general and of computer terrorism, in

197. Доклад Центра защиты национальной инфраструктуры ФБР США
Centre for Protection of the national infrastructure of the U.S. FBI.
198. Количество пользователей Интернета в России за последние 5 лет утроилось
Internet users in Russia over the past 5 years has tripled.
199. Окинавская хартия глобального информационного общества. Принята 22 июля 2000 г.
particular. They are high latency and low level of detection. The Head of the Department of Special Technical Russian Interior Ministry, Colonel-General Police, Boris Miroshnikov notes that “... the information weapon may be selective. It can be used in cross-border links, which may make it impossible to identify the source of the attack. Therefore, information weapons may be an ideal tool for terrorists, and information terrorism may become a threat to the existence of entire nations, which makes the issue of information security an important aspect of national and international security, and the role of this aspect will only increase.”

According to Interpol estimates, the growth rate of crimes, such as Internet crime, is the fastest on the planet. Thus, the Interior Ministry believes that the Internet now has “more than 4800 sites belonging to different extremist organizations, while only fifteen years ago there were only 12.” (Urazbaev) According to the Council of Europe experts, losses from cyber attacks and viruses are about 12 billion, and the violation of property rights is detrimental to the $250 billion.

The novelty of the problem caught the police unprepared. They were not ready to adequately fight and control this new socio-legal phenomenon. At present, the issue of computer crime and cyber-terrorism, is out of the control of law enforcement agencies and has developed into a serious state and international problem. Terrorists use computers and the Internet for terrorist activities. This includes communication with each other, planning, finding money, intelligence gathering, recruitment and distribution of promotional materials.

From the standpoint of national security in this area there is a dangerous trend of increasing technical and technological dependence of the state. Richard Clarke (former coordinator of security, infrastructure protection and counterterrorism National Security Council, United States) indicates a potential terrorist use of computer systems and capabilities for attempts to breach the critical infrastructures. According to experts, terrorism, using the latest advances in high technology is no less dangerous than nuclear or biological terrorism.

The term “cyberterrorism” was introduced in the mid-1980s by Barry C. Collin in order to identify terrorist activity in cyberspace. The author of the term

---

201. Там же. Ibid.
suggested that the real cyber terrorism could be foreseen no earlier than in the first decade of the 21st century, but the first cyber attack was recorded in the early 1990s.

Researchers M.J. Devost, B.K. Houghton, N. Pollard identified information terrorism, which is the expression of cyberterrorism as:

1. connection of criminal use of information systems by means of fraud or abuse to physical violence inherent in terrorism;

2. deliberate abuse of digital information systems, networks or components of these systems or networks in order to facilitate the implementation of terrorist operations or acts. 204

In 1996, FBI Special Agent M. Pollitt proposed a definition of cyber-terrorism: “The deliberate, politically motivated attack against information, computer systems, computer programs and databases in a violent invasion by international groups or secret agents.”

Because computer terrorism is a reality, it is imperative that it be addressed nationally and internationally so that responsibilities for prevention, response to and eradication of this form of terrorism. Protection of computer networks and their operations is considered to be one of the most significant yet vulnerable elements within both U.S. and Russian society. It is important to assess and analyze the nature and characteristics of cyberterrorism and a means of developing and definition and then subsequent control strategies as effective tools in the prevention of this crime.

In the Russian legal literature, the necessary definitions related to this act are very vague. Within Russian legal science, there are two basic approaches to the concept of cyber-terrorism. According to the first, the concept of cyberterrorism is defined based on a set of symptoms associated with the acts (attack or threat of attack) against computers, networks or information. D. Denning considers cyberterrorism as the unlawful attack or threat of attack on computers, networks or information found in them, perfect in order to force the authorities to help achieve political or social objectives. 205 A. Rubanov believes that cyberterrorism is a premeditated, politically motivated attack on legally protected information in critical segments of the state, as well as the private sector, provided in electronic format on computer media, with the criminal use of information systems, creating a risk of death, cause significant property damage,


or other socially dangerous consequences or threat to commit such acts in order to terrorize.206

A similar position is held by A. Urazbaev,207 Y. Gavrilov 208. An approach, similar to that of the Russian definitions, discussed in the previous paragraph, has been implemented in the new U.S. Anti-Terrorism Law known as Act of 2001.209 For the first time, this law introduces the concept of “cyberterrorism” into the legal cannon. Cyberterrorism involves various forms of hacking qualified and prejudice-protected computer networks of citizens, legal persons and public agencies, including damage to the computer system used by the government department in the organization of national defense or national security.

The second approach to the definition of “cyberterrorism” focuses on the nature of these targeted actions. R. Gereev210 and V.A. Mazurov propose that cyberterrorism include acts that are intended to intimidate the population and authorities, in order to achieve criminal intent, manifested in the threat of violence, maintaining a constant state of fear with the motivation of political or other purposes, forcing certain actions, to draw attention to the individual cyberterrorists or terrorist organization, that it represents.

V.A. Mazurov argues that it is necessary to differentiate between damage to computer systems and cyber-terrorism.211 The scientist calls cybercrime the wrongful interference with the operation of computers, computer software, computer networks, unauthorized computer data, as well as other socially dangerous illegal acts committed on or through the computer, computer networks and software crime committed in cyberspace. By the term “cyber-terrorism,” V.A. Mazurov means the disruption of information systems, intimidating the population and pose a risk to life, causing significant property damage or other serious consequences, in order to influence decision-making authorities or
international organizations, as well as a threat to commit such acts in the same order.

A number of other authors believe that cyberterrorism consists of a series of illegal activities in cyberspace, involving the attempt on the lives of people, threatening reprisals, destructive actions with regard to material objects, distortion of objective information, or some other action to facilitate whipping up fear and tension in society in order to gain an advantage in dealing with political, economic or social problems. Defining cyberterrorism as a series of cybercrimes conducted with the goal of maintaining a state of fear (through intimidation), is more useful for differentiating cyberterrorism from similar, but less socially dangerous actions.

Informational interference as an act of terrorism is different from other actions in cyberspace, especially in its objectives, which are characteristic of the political act of terrorism. Cyberterrorism focuses on the use of various forms and methods for the decommissioning of the information infrastructure of the state or by the use of the information infrastructure to create an environment that leads to disastrous consequences for society and the state. There is a direct correlation between the degree of development of information infrastructure, the computerization of the country and the number of cyber terrorist acts. The present challenge of cyber terrorist acts is relevant for countries that are leaders in the field of satellite communication systems and global networks.

The primary means of engaging in a terrorist attack within the realm of technology is an attack on computer information, computer systems, data transmission equipment, and other components of information infrastructure, performed by groups or individuals. Such an attack can penetrate into the target system, intercept control or suppress a means of information exchange network, to carry out other destructive actions. In cyberspace, there are also various techniques for the commission of a terrorist act:

- Damage to the individual elements of cyberspace, the destruction of power supply networks, conducted emissions, the use of special programs that promote the destruction of hardware;
- Theft or destruction of information, software and technical resources of cyberspace that are of strategic importance; overcoming security systems, introducing viruses, software bookmarks;
- Altering software and information such that it results in the destruction or modification of information and management systems, and the threat of disclosure or the publication of classified information on the operations of the information infrastructure of the state, public interest and military information systems, encryption codes, principles of encryption systems;

Capture channels from broadcasting telecommunications in order to spread disinformation, rumors, demonstrate the power of a terrorist organization and their ad claims;

The destruction and suppression of active links, incorrect addressing, artificial congestion node communication, the impact on operators, developers, information and telecommunications systems to commit their actions listed above.\textsuperscript{213}

An example of cyber-terrorism with the use of modern information technology is the computer virus, dubbed “I love you”, launched on the Internet. It spread across the globe, at an incredible rate, disrupting the work of government agencies, computer networks and corporate parliaments of many countries. Having received, over the Internet, unauthorized access to networks of organizations and overcome a number of locks and security barriers, hacker attacks, the virus produces a reconfiguration of the systems, resulting in completely blocked information data. “I love you” is the fastest computer virus of any that have existed to date. Experts warn that because of the ability to “mutate”, it can increase its destructive potential. According to the estimates of the analytical group, Cyber Day Systems, the virus “I love you” is the most serious known act of cyberterrorism in history.\textsuperscript{214}

At present, the current developing circumstances require urgent improvement and development of the existing system of counteraction against terrorism as a holistic, integrated structure that would combine actions against terrorism on all fronts, anticipating new manifestations of these cyber acts. One tool for countering cyberterrorism is to develop enabling national and international legislation. In both Russia and the United States, the existing international laws are insufficient. There is the need for an adequate response to this threat through legislation.

Under Russian law, cyberterrorism can be defined by connecting the concepts of “cyberspace” and “terrorist act” (in accordance with Article 205 of the Criminal Code). As such, cyberterrorism is a deliberate attack on computers, software, computer network or their processed information, creating a risk of death, cause significant property damage or other socially dangerous consequences. This action must be taken to disturb public security, intimidating the population or to influence the decisions of the authorities. This type of terrorism may also include a threat of committing such acts in order to achieve these goals.


An amendment to Part 2, Art. 205 of the Criminal Procedural Code has been proposed that would strengthen the criminal responsibility for terrorism involving computer information, computer, computer system or computer network. Then, using the respective additions of other articles of the Penal Code, relating to terrorist activities, it will be possible today to qualify cyber-terrorism as a crime against public security and public order under the national law of the Russian Federation.

With the exception of the United States, cyberterrorism has not been defined in national legislation. This is problematic as the victims of cyber terrorists are specific countries and, as with general jurisprudence, punishment must be applicable for this crime in all nations but most importantly in those nations that have the greatest risk of victimization. Similarly, the national and international laws must provide for the global nature of terrorism. Cyber-terrorism (and its progenitor - terrorism) - is a crime against humanity and such acts should be judged by universal standards. This requires an international approach and legislation that can coordinate and promote legal actions across national jurisdictional boundaries. Currently, the complexity of disparate laws internationally makes the investigation and prosecution of this crime extremely difficult.

In Russia’s view, the existing international legislation and, most importantly, the Council of Europe Convention on Cybercrime in 2001, is not sufficient to counter the actions of these terrorists who are becoming more sophisticated and ambitious. Russia has offered to develop a global strategy to combat cyberterrorism for the global community. Undoubtedly, the main role in the fight against cyberterrorism must belong to the nation-states. At the instigation of the Russian Federation, the UN General Assembly adopted a resolution on cybercrime, cyberterrorism, and cyberwar. The resolution calls upon Member States to inform the UN Secretary-General of their views and assessments on: (1) the issues of information security; (2) the definitions of basic concepts related to information security; and (3) the development of international principles, improving the global information space and telecommunications and to help combat information terrorism and criminality.

Laws, practices and policies are evolving to address the new cyber world, as further evidence by the May, 2011 publication of the International Strategy for Cyberspace of the U.S. government. The parameters of these areas will evolve over time, leading, perhaps, to such as final characterizations of the Stuxnet malware deployment against Iran. The publication of the Manual on

216. Id. at ¶ 10.
International Law Applicable to Cyber Warfare (also known as the Tallinn Manual), sponsored by the North Atlantic Treaty Organization Cooperative Cyber Defense Programme, will help define these parameters and create a framework for them.

6. The Global Framework

The transnational nature of cybercrime creates many challenges. The conformance of law promoted by the Convention on Cybercrime is the beginning and the basis for promoting the cooperation necessary to combat cyberterrorism. The idea that criminal justice methods might apply to cybercrime and information security systems was introduced by the Institute for Strategic Studies of the U.S. Army War College. The enmeshed nature of cyber networks assures that addressing cybercrime may impact civil society where a response to a cybercrime, particularly one of cyberterrorism or hostile state action, create “profound constitutional and security challenges” for the United States. Id. The National Cyber Leap Year Co-Chairs Report addressed the need for “game changing” approaches as current thinking on cyber security is inadequate to protect people from cybercrime.

Safety and security require more than technical protections and police response. They necessitate critical blend of technical protections and legal response with individual practice and social norms. Ways of controlling and limiting injurious behavior, whether formal or informal, are essential for public safety. A strong community will have both. These must be incentivized and empowered at all levels. But the challenge of this in a transnational computing world is of an entirely new order.

Routine activity theory/opportunity theory and displacement theory, which are used to study deviant behavior in physical communities, may offer ways to examine ways of informal social control on cyber security and control cybercrime. Routine activities theory ("RAT") asserts that three main factors

can impact criminal conduct: (1) a suitable target, (2) a lack of guardianship, and (3) a motivated offender.\textsuperscript{224} The absence of one of these elements reduces the opportunity for deviant behavior but the presence and convergence increases it.

This analysis may also be applied to cybercrime and security. Social control is a function of both formal and informal social control\textsuperscript{225}. Laws, public policies, and law enforcement exemplify elements of formal social control, whereas community attitudes and norms exemplify informal social control. In cyber security contexts, high levels of informal social control are essential to deter cyberattacks, particularly since attackers exploit the anonymity and distance-collapsing features of cyberspace as vectors for attack.

Open source software a collaborative social network that self-organizes and grows as a preferentially-attached network.\textsuperscript{226} Online social networks themselves suggest opportunities for the examination of RAT-based security promotion. For instance, Mislove, et al. found that online social networks have power-law, small-world and scale-free properties; these would indicate potential for expansion of a guardian security regime.\textsuperscript{227}

RAT can be applied to criminal activity involving computing systems but the variations with live time may still limit its effectiveness.\textsuperscript{228} Degradation in a social network and member participation may reduce the protective elements of the participants.\textsuperscript{229} And masked attacks may simulate normal activity to subvert protective activity.\textsuperscript{230} Nonetheless these criminal justice models may offer opportunities to mitigate cybercrime’s impact on information society.
Another possibility might be, in effect, a transnational court using the transnational technologies at issue. One example of this is the introduction of IP based arbitration courts in the Russian Federation. The introduction of new technologies in the work of state bodies resulted in three sets of rules that entered into force in 2010. They govern the use of the Internet, audio protocols (reporting) and videoconferencing in arbitration courts of Russia. The adoption of the Russian Federation Law of 27.07.2010 № 228\(^{231}\) made possible participation of parties to the hearing via video-conferencing.

In order to use video-conferencing, an individual must submit an application.\(^{232}\) This application has the following characteristics: (1) It is submitted to the court hearing the case; (2) It is submitted before its appointment to the proceedings; (3) It is considered by a single judge within five days after the date of receipt in court; (4) It is considered without notice to the parties; and (6) It indicates the court of arbitration, with the assistance of which the applicant may participate in the hearing through video conferencing.\(^{233}\)

Such a petition may be also declared in the claim or in the recall of claim. It should be noted that the ruling of the arbitral court to dismiss the petition under consideration is not subject to appeal (Part 1 of Art. 188 APC, paragraph 24 of Resolution of the Plenum of the RF on February 17, 2011 N 12). It is not the responsibility of the person claiming such a petition to ascertain whether there is technical feasibility of video conferencing in this arbitration. The court satisfies or fails to meet the petition (Section 1 Part 5 of Art. 1531 of the APC), taking into consideration the legal proceedings.

The grounds for refusal of this application are lack of technical capacity to participate in the hearing with the use of video conferencing, as well as proceedings before a closed court session. In practice, there is a general assumption that the absence a special court order, due to which a claimant may participate in the hearing will result in the denial of the application to participate in the hearing through the use of videoconferencing systems. Moreover, given Part 5 of Art. 159, an arbitration court may refuse the application or petition, if they have not been timely filed by a person involved in the case, due to abuse of procedural law and are clearly aimed at disrupting the hearing, the delay of the trial, preventing consideration of the case and take legal and informed the court act, except if the applicant had no opportunity to file a claim or a request earlier for objective reasons.

---

231. Арбитражный процессуальный кодекс РФ от 27.07.2010 № 228

232. АРИБТРАЖНО-ПРОЦЕССУАЛЬНЫЙ КОДЕКС РОССИЙСКОЙ ФЕДЕРАЦИИ [АПК РФ] [Code of Arbitration Procedure] art. 159, part 4 (Russ.).

233. Id.
Under Part 2 of Art. 153.1 of the Code of Arbitration Procedure\footnote{234. Арбитражный процессуальный кодекс РФ от 27.07.2010 № 228 www.consultant.ru/popular/apkrf/ (The Russian Federation Code of Arbitration Procedure).} if the application is accepted by the court, the Arbitration Court requests that the arbitral tribunal, with the assistance of which the applicant will be able to participate in the hearing, to arrange the organization of video conferencing due to a decision based on the court order in accordance with Art. 73 of the APC. It is mandatory for the arbitral tribunal, which was instructed, and must be completed no later than 10 days from the date of receipt of a copy of the court decision.

If the petition had stated the need in the VCC, but it came after the approval date of the preliminary hearing, in accordance with Part 4 of Art. 137 (assignment of the case to trial) it is impossible to go from the preliminary hearing to the main hearing, otherwise it violates the right of parties to judicial protection. If the case is opened, the parties shall receive an adequate decision, which indicates what action they should take and what evidence is to be present.

In accordance with Part 4 of Art. 153 of the Code of Arbitration Procedure by using videoconferencing systems in the two courts of arbitration shall be drawn up and is recording the hearing. Video of the hearing on a physical medium, within five days is to be sent to the court hearing the case, and attached to the minutes of the hearing.

The protocol drawn up by the court, arranging videoconferencing, indicates the date and place of the hearing, the name and case number, information about the persons involved in the case, their representatives and other participants in the arbitration process, as well as a notation on the use of video conferencing. The protocol signed by the secretary or assistant trial judge, assisting in the organization of the judicial process, the protocol and written evidence presented at trial, together with a material carrier are sent to the recording sessions court hearing the case and placed in the materials of the case (Part 2 of Art. 74). In conclusion, we note that the introduction of the regulations to conduct the hearing by the use of videoconferencing systems will certainly help to achieve justice in arbitration courts - ensuring access to justice in the sphere of entrepreneurial and other economic activity and fair public hearing within the statutory time by an independent and impartial tribunal. We believe that, over time, lawmaking and judicial practice in this area negate all the shortcomings in this regard.

This type of system may help overcome the political-jurisdictional issues seen in the Ivanov and Gorshkov hacking prosecutions. That transnational investigation and prosecution under the Computer Fraud and Abuse Act alleged the widespread hacking computers in the United States by operators in Western Russia using Internet links.\footnote{235. United States v. Ivanov, 175 F. Supp. 2d 367 (D. Conn. 2001).} While a U.S. court found key elements met by the
technology, the jurisdictional problem was handled in an old-fashioned way: the federal agents convinced the Russian perpetrators to come to the United States for what was, in effect, a “job interview” on computer security. But the U.S. federal agents also used a key logger to acquire information they used to log back into Ivanov’s computer in Russia and download significant incriminating evidence. These actions were without the permission of Russian authorities and thereby damaged U.S.-Russia relations in this area. A system for addressing such transnational problems while demonstrating respect for sovereignty might avoid confusion and encourage the cross-border cooperation that is necessary to enforce laws against cybercriminals.

IV. CONCLUSION

Cybercrime demands evolving responses in law, technology and fact. To the extent we hope to protect our citizens, in both their persons and their liberties, rather than just respond to depredations, we must be creative. The amazing communication and computing powers of the modern world have led to surprising crimes where victims and perpetrators may be separated by thousands of kilometers and whole disciplines of knowledge. These offenses must be addressed. How we do so depends on adaptation and attention to the requirements of public safety and due process. That we must consider them in a global context is a great challenge, but also extends the great promise of these technologies to bind the world together. Properly done, these technologies will help truly make the fair administration of justice a global expectation that protects everyone.

236. Id. at 371-72 (“At the point Ivanov gained root access to OIB's computers, he had complete control over that data, and consequently, had possession of it. That data was in OIB's computers. Since Ivanov possessed that data while it was in OIB's computers in Vernon, Connecticut, the court concludes that he obtained it, for purposes of § 1030(a)(4), in Vernon, Connecticut. The fact that Ivanov is charged with obtaining OIB's valuable data by means of a complex process initiated and controlled from a remote location, and that he subsequently moved that data to a computer located in Russia, does not alter the fact that at the point when Ivanov first possessed that data, it was on OIB's computers in Vernon, Connecticut.”).
REGULATING HUMAN SUBJECTS RESEARCH IN THE INFORMATION AGE: DATA MINING ON SOCIAL NETWORKING SITES

Lauren B. Solberg*

In the 1970s, the Department of Health, Education & Welfare promulgated the first regulations governing research with human subjects. Currently, the Department of Health and Human Services regulates both biomedical and behavioral research with human subjects through 45 C.F.R. § 46, but these regulations have not been revised to address the advances in technology that have changed the ways in which human subjects research is conducted in the 21st century. One of these advances includes researchers’ use of the Internet for various research purposes, including recruiting subjects for their studies, as well as mining data on social networking sites. The issue of data mining on social networking sites for research purposes is becoming more important as researchers in a number of academic fields are collecting research data in this manner. The question of whether such research involves “human subjects” as the term is defined in 45 C.F.R. §46 is important because the answer dictates whether or not such research is subject to federal regulation and oversight.

The U.S. Department of Health and Human Services’ Office for Human Research Protections (OHRP) has previously acknowledged an increased use of the Internet for research purposes, but it has not published any guidance about how the Office understands the issue (nor have any applicable specific regulations been promulgated). Such guidance, and particularly guidance that addresses the use of social networking sites for research purposes, is becoming increasingly more important as researchers are expanding beyond just Facebook and MySpace to recruit research participants and collect data. Furthermore, new social networking sites such as PatientsLikeMe.com are changing the ways in which both behavioral and biomedical researchers recruit and interact with study participants.

This Article identifies three key research activities that any new guidance that the OHRP publishes about Internet research should address: (1) the use of the Internet (including social networking sites) to recruit subjects; (2) the use of the Internet to collect personal information via direct interaction with site users; and (3) the collection of personal information from the Internet for research purposes without direct interaction with the owner of the information, i.e. data mining. It further explores recent case law

* Assistant Vice President of Human Subjects Protection & Research Integrity, Meharry Medical College, Nashville, TN. J.D., Vanderbilt University; M.T.S., Harvard University; B.A., University of Florida. The author is grateful for the thoughtful comments and questions from the participants of the Northern Kentucky University Law Review Law & Informatics Symposium which contributed to the final version of this article. The author also wishes to acknowledge the editorial assistance of Adam Shniderman with this article. This work was supported in part by Meharry R-Center grant 5 U54 RR026140-03 (NCRR)/8 U54 MD007593-03 (NIMHD), Vanderbilt CTS4 grant 5UL1 RR024975 (NCRR), and 3S21MD000104-11S1 (NIH/NIMHD).
that says that there is no reasonable expectation of privacy with respect to information posted on social networking sites, and discusses the history of privacy in the federal regulations governing research with human subjects. This Article concludes that in light of the changes in online social networking and resulting changes in expectations of privacy, as well as the consideration that the Department of Health and Human Services is giving to revising 45 C.F.R. § 46, guidance – or even new regulations – should be drafted that address these key research activities. It furthermore suggests language that would inform researchers and research institutions whether each of these key research activities is subject to the regulations governing research with human subjects.

I. INTRODUCTION

The Internet, and specifically the prevalence of social networking sites like Facebook, Twitter, and MySpace, has greatly changed the landscape of human subjects research.1 When 45 C.F.R. § 46, the federal regulations that govern the conduct of research with human subjects, was first promulgated in 1974, the Department of Health, Education & Welfare (HEW) could not have anticipated the ways in which the use of a computer would affect the conduct of human subjects research in the future. At that time, protecting an individual’s private information that might be revealed during the course of research appeared only to be of general concern to HEW.2 Instead, media attention was focused on the revelation to the American public of the U.S. Public Health Service study of syphilis in Tuskegee, Alabama, often referred to as the Tuskegee syphilis study.3 Between 1932 and 1972, approximately 400 African-American men in Alabama with syphilis were left untreated by U.S. government researchers who wanted to understand the course of the disease.4 The regulations were promulgated in large part in response to this atrocity, and were initially intended to protect individuals against unnecessary risk that they might incur during the course of their participation in biomedical research.5

The regulations have evolved over time to seek to protect against any number of risks that participants in biomedical as well as in behavioral and

1. See infra Part III.
2. Contrary to today, where a “human subject” is – among other things – one about whom a researcher obtains identifiable private information, no mention of privacy exists in the 1974 regulations. See 45 C.F.R. §46.102(f) (defining a “human subject” in research); infra Part II discussing the history of the regulations governing human subjects research.
4. Jean Heller, Syphilis Victims in U.S. Study Went Untreated for 40 Years, N.Y. TIMES, July 26, 1972, at 1, 8.
5. See Secretary’s Interpretation of “Subject at Risk,” 41 Fed. Reg. 26572 (June 28, 1976) (explaining that “[t]he regulations were not, and have never been, intended to protect individuals against the effects of research and development activities directed at social or economic changes...”). See also infra Part II for a discussion of the history of the regulations governing human subjects research.
social science research may incur, and have evolved to provide special protections for vulnerable populations in research. However, the last time that Subpart A, the provisions in 45 C.F.R. § 46 that govern research with all human subjects, was revised was in 1991. The dated nature of these regulations necessarily means that they specifically do not take into account developments in technology, such as the Internet, that have changed both people’s perceptions of privacy as well as the general conduct of human subjects research.

The fact that changing perceptions of privacy in conjunction with recent technological advancements are not accounted for in 45 C.F.R. § 46 often makes it difficult to interpret the regulations as currently written, and in particular makes it difficult to determine when human subjects are involved in research when that research involves the use of the Internet. A human subject is “a living individual about whom an investigator (whether professional or student) conducting research obtains (1) [d]ata through intervention or interaction with the individual, or (2) [i]dentifiable private information.” Private information is identified as “information about behavior that occurs in a context in which an individual can reasonably expect that no observation or recording is taking place, and information which has been provided for specific purposes by an individual and which the individual can reasonably expect will not be made public (for example, a medical record).” Because the identification of research as “human subjects research” may hinge on whether private information is being obtained about a living individual, it is important for researchers and Institutional Review Boards (IRBs), committees charged by 45 C.F.R. § 46 to review research with human subjects, to know when private information is being obtained. The ability


7. 45 C.F.R. §46 (2011). While Subpart A pertains to research with all human subjects, Subparts B, C, and D of 45 C.F.R. §46 govern research with pregnant women and fetuses, prisoners, and children, respectively. Id. Subpart A is often referred to as the “Common Rule.” See infra note 194.

8. See discussion infra Part III (describing different ways that the Internet is used in research).


10. Id.

11. The IRB is a committee typically composed of faculty, staff, and/or students at a research institution that reviews all human subjects research to ensure that it is both ethical and compliant with these federal regulations. See 45 C.F.R. § 46.107 (2012) (stating the requirements for IRB membership). Once constituted, the IRB reviews the research to determine whether subject selection is equitable, whether the risk is proportional to the benefits, and whether the confidentiality of any data that are collected will adequately be protected. 45 C.F.R. § 46.111 (2012) (detailing the criteria that the IRB must confirm are satisfied before approving a project).
to make this determination is more difficult in our technological age, and requires an understanding of when individuals have a reasonable (or unreasonable) expectation of privacy.

Unfortunately, the Office for Human Research Protections (OHRP), the office in the Department of Health and Human Services (HHS) (formerly HEW, until 1980) that interprets and enforces 45 C.F.R. § 46, has published almost no guidance or other informal advice, e.g., in the form of a letter or list of FAQs, about the use of the Internet in human subjects research.12 Without input from HHS through informal rulemaking or other means, researchers and IRBs are left to interpret the current regulations themselves when it comes to respectively designing and reviewing studies that involve the use of the Internet. Because the use of the Internet is prevalent in biomedical, social, and behavioral research studies,13 there are countless numbers of researchers – not just researchers in one particular field or type of field – who would benefit from new regulations or guidance that clarify when research facilitated by the Internet is human subjects research.

This article focuses in particular on one way in which the Internet is used to conduct research – data mining on social networking sites. With the increasing prevalence of the use of social networking sites, academic researchers have realized the vast amount of data that exist to be analyzed, so predictably they are logging on to these sites and reviewing the information that people post in order to draw various conclusions about human thought and behavior.14

While some uses of the Internet are more clearly used to facilitate human subjects research, or are, in and of themselves, human subjects research as defined in 45 C.F.R. § 46,15 it is not entirely clear whether researchers who collect data for a study solely by mining social networking sites are engaging in research with “human subjects” as defined in 45 C.F.R. § 46.102(f). This is in large part because of changing notions of privacy. My previous work analyzed the definition of a human subject, focusing on whether data mining on social networking sites like Facebook is research with human subjects and, as such, is

12. See United States Department of Health and Human Services, Policy and Guidance Index, http://www.hhs.gov/ohrp/policy/index/index.html (last visited Aug. 9, 2012). The only information that the OHRP has made available online regarding Internet research is this guidance document that discusses what IRBs should look for when reviewing advertisements published on clinical trials web sites. See infra text accompanying note 63. Although helpful, this single document does not begin to address the numerous other ways in which researchers use the Internet to facilitate their research, e.g. for distribution of surveys, or for visits to chat rooms. See discussion of such uses of the Internet to facilitate the conduct of human subjects research infra Part III.A.
13. See infra Part III.A. for a discussion of the ways the Internet is used for research.
14. See infra Part III.B. for a discussion of data mining on social networking sites.
15. 45 C.F.R. § 46.102(f).
federally regulated. Furthermore, my previous work analyzed what type of IRB review would be required if 45 C.F.R § 46 regulates this type of research.

This prior work concluded that data mining on social networking sites likely does not involve a researcher obtaining data about an individual through intervention or interaction. However, this is only true as long as that researcher does not actively communicate with the individual for purposes of collecting data, for example, there is no verbal exchange, either online or in person, between the two parties. Such research is also not human subjects research if the researcher does not “friend” the individual for the sole purpose of collecting research data. Furthermore, and more importantly for the purposes of this article, I concluded that information posted by individuals on social networking sites likely is not private because, under most circumstances, people can no longer have much reasonable expectation of privacy with respect to information they post online, especially on a social networking site. However, the issue of what “private information,” as used in 45 C.F.R. § 46, is in light of the technology readily available today is still unresolved.

Part II of this article discusses the history of privacy in the federal regulations that govern human subjects research. Part III describes the ways in which researchers make use of the Internet for their research, and affirms my earlier conclusion that one of these ways – data mining on social networking sites – likely is not human subjects research, primarily because individuals have a very limited expectation of privacy when it comes to information they post online. Part IV examines how courts view individuals’ expectations of privacy with respect to the information they post on social networking sites, and Part V identifies a new type of social networking site that is being used for academic research purposes. In light of the static federal regulations governing human subjects research, the technology that is readily available to researchers, and the limited expectations of privacy that people have on the Internet, Part VI suggests language for new regulations or guidance that address Internet research.

17. *Id.*
18. *Id.* at 321, 324.
19. *Id.* at 324.
20. *See id.* at 321, n.70.
21. *Id.* at 328.
22. The United States Food and Drug Administration (FDA) held public hearings in 2009 to explore the possibility of developing policy or guidance on promoting FDA-regulated products on the Internet and through social media. U.S. Public Hearing on Promotion of FDA-Regulated Medical Products Using the Internet and Social Media Tools, Food and Drug Administration, (Nov. 12-13, 2009), http://www.fda.gov/AboutFDA/CentersOffices/OfficeofMedicalProductsand Tobacco/CDER/ucm184250.htm. The only publication to date is draft guidance published in December 2011 entitled “Responding to Unsolicited Requests for Off-Label Information About Prescription Drugs and Medical Devices” that mentions social media and the Internet, but was not issued for the specific purpose of addressing social media and the Internet. Draft Guidance on Unsolicited Requests for Off-Label Information, EYE ON FDA, http://www.eyeonfda.com/
II. A HISTORY OF PRIVACY IN 45 C.F.R. § 46

Interpreting the meaning of “private information” as defined in 45 C.F.R. § 46.102(f) requires an understanding of what reasonable expectations of privacy are, and in particular, what they are in light of today’s technology. What were considered reasonable expectations of privacy at the time of the initial promulgation of 45 C.F.R. § 46 in 1974, or even in 1991 when Subpart A was last revised, may no longer be applicable. Indeed, “privacy must be evaluated in light of the ‘modern enterprise and inventions’” and while “[i]t is still possible to protect privacy, [d]oing so requires that we rethink outdated understandings of the concept.” Thus, it is reasonable for IRBs to believe that some research facilitated by the Internet involves the collection of private information; however, we cannot continue to apply the same standards for determining whether that information is private – particularly when it is collected from social networking sites.

As previously mentioned in the Introduction, the current federal regulations governing research with human subjects define a human subject as “a living individual about whom an investigator (whether professional or student) conducting research obtains (1) data through intervention or interaction with the individual, or (2) identifiable private information.” The regulations then explain that “[p]rivate information includes information about behavior that occurs in a context in which an individual can reasonably expect that no observation or recording is taking place, and information which has been provided for specific purposes by an individual and which the individual can reasonably expect will not be made public (for example, a medical record).” These definitions are found in Subpart A of the regulations, which underwent its most recent revision in 1991; however, the definitions of a human subject and private information have remained static since a 1981 revision of the regulations.

These definitions are found in Subpart A of the regulations, which underwent its most recent revision in 1991; however, the definitions of a human subject and private information have remained static since a 1981 revision of the regulations. An in-depth examination of the evolution of the definition of a human subject in 45 C.F.R. §46 shows how HHS came to seek protection of

---

25. 45 C.F.R. § 46.102(f).
26. Id.
27. See Final Regulations Amending Basic HHS Policy for the Protection of Human Research Subjects, 46 Fed. Reg. 8366, 8387 (Jan. 26, 1981) (to be codified at 45 C.F.R. pt. 46) (defining “human subject,” which is the same definition that is currently found at 45 C.F.R. § 46.102(f)).
individuals whose identifiable private information is obtained during the course of research, what HHS believed to in fact be private information, and why clarification of what private information is would assist researchers and IRBs in conducting and reviewing research involving the Internet.

When 45 C.F.R. § 46 was first promulgated in May 1974, the regulations reflected the same fundamental purpose that they do now – to protect individuals enrolled in research. However, the notice of proposed rulemaking published in 1973 and the final rule published in the Federal Register in 1974 reveal that the concepts of privacy and private information were not specific concerns of HEW.28

While a “human subject” now is defined in the regulations, the 1974 regulations did not contain such a definition.29 Although HEW’s explanation of the final rule discussed the involvement of “human subjects” in research, and although the regulations themselves used the term “human subject,” the first set of federal regulations protecting human subjects in research failed to actually define a “human subject.”30 Instead, these regulations only defined a “subject at risk,” which was

any individual who may be exposed to the possibility of injury, including physical, psychological, or social injury, as a consequence of participation as a subject in any research, development, or related activity which departs from the application of those established and accepted methods necessary to meet his needs, or which increases the ordinary risks of daily life, including the recognized risks inherent in a chosen occupation or field of service.31

There was no mention of privacy or private information at all in either the notice of proposed rulemaking or in the final rule.32

A notice subsequently published in the 1976 Federal Register explained this omission to a certain extent. The notice provided the HEW Secretary’s interpretation of a “subject at risk,” indicating that the regulations as promulgated in 1974 were designed to protect people against harms suffered in biomedical research, citing harms such as those that could be suffered as a result of experimentation with “FDA-approved drugs for any unapproved purpose; psycho-surgery and other techniques for behavior control currently being developed . . . use of experimental intrauterine devices; [and] biomedical

30. See id.
31. Id. at 18917.
research in prison systems..." The Secretary specifically states that “[t]he regulations were not, and have never been, intended to protect individuals against the effects of research and development activities directed at social or economic changes, even though those changes might have an impact upon the individual.” Thus, protecting against the disclosure of a person’s private information that was learned during the course of research was not a specific goal of the regulations.

It was not until 1978 when the National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research (the National Commission), in accordance with its charge in the National Research Act to study IRBs, issued a report and recommendations about IRBs that there was any recognition on the part of the government that private information obtained during the course of research may require special protection. The National Commission’s report on IRBs included a definitions section, and the current regulatory definition of a human subject was derived from this report. The National Commission defined a human subject as “a person about whom an investigator (professional or, student) conducting scientific research obtains (1) data through intervention or interaction with the person, or (2) identifiable private information.” The National Commission went on to elaborate on the meaning of private information, commenting that

‘[p]rivate information’ includes information about behavior that occurs in a context in which an individual can reasonably expect that no observation or recording is taking place, and information which has been provided for specific purposes by an individual and which the individual can reasonably expect will not be made public (e.g., a medical record). Private information must be individually identifiable (i.e., the identity of the subject is or may readily be ascertained by the investigator or associated with the information) in order for obtaining the information to constitute research involving human subjects.

34. Id.
35. Institutional Review Boards: Report and Recommendations of the National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research, 43 Fed. Reg. 56174 (Nov. 30, 1978). This report issued by the National Commission should not be confused with the Belmont Report, one of the most well-known discussions of the ethical principles that should govern research with human subjects. The Belmont Report, which identified the three fundamental principles of research ethics as respect for persons, beneficence, and justice, was not published in the Federal Register until 1979. Belmont Report, 44 Fed. Reg. 23192 (Apr. 18, 1979).
36. Id.
38. Id.
The language that the National Commission used to explain private information is now included in 45 C.F.R. § 46.39 Thus, the only differences between the National Commission’s definition of a human subject and the current definition in 45 C.F.R. § 46 are that the current regulations define a human subject as a “living individual,” and the current regulations do not limit the scope of the definition to “scientific research,” instead seeking to protect participants in simply “research.”40

Following the National Commission’s publication of their report on IRBs, HEW’s proposed amendments to 45 C.F.R. § 46 sought to include a definition of a “human subject” for the first time rather than simply a “subject at risk,” 41 though the definition at that time did not as closely resemble the definition that the National Commission provided in its report on IRBs.42 HEW instead proposed to only define a human subject as “an individual about whom an investigator (whether professional or student) conducting research obtains (1) data through intervention or interaction with the person, or (2) identifiable information.”43 Thus, the proposed amendments excluded the term “private” from the definition of a human subject even though the National Commission had expressed concerns about IRBs reviewing the ways in which private information might be used in research.44 Additionally, a final rule was published in April 1979 allowing for the issuance of certificates of confidentiality under the Public Health Service Act to shield the identity of individuals enrolled in mental health research (further emphasizing the importance of protecting privacy and confidentiality in research).45

The HHS explanations provided in the publication of the final rule in 1981 stated that there were fewer than twenty comments submitted to HHS about the proposed definition of a human subject, with some objecting to the broad nature of the definition, indicating that the protection of subjects of non-biomedical research (i.e., subjects of social or behavioral research) under the regulations

39. See 45 C.F.R. § 46.102(f).
would be unnecessary.\textsuperscript{46} However, in an effort to comport with recommendations proffered by the National Commission, the agency chose to adopt the National Commission’s definition of a human subject, making only a few minor changes,\textsuperscript{47} and this definition is the one included in the regulations today.\textsuperscript{48} By including the term “private” in the definition of a human subject, HHS anticipated that the definition would “exempt[] from the regulations nearly all library-based political, literary and historical research, as well as purely observational research in most public contexts, such as behavior on the streets or in crowds.”\textsuperscript{49}

Of course, HHS could not have conceived of the Internet as a commonly used research tool in academia in the 1970s or early 1980s, much less anticipated it as a means of data collection. However, the shift in HHS’s thinking about risk to participants in research, and its resulting shift in its view of who really requires protection as research subjects is an interesting one. HHS took seriously the recommendations of the National Commission in an effort to ensure better protections for human subjects in research.\textsuperscript{50} However, the agency has not revised its definition of a human subject or elaborated on the notion of identifiable private information since the 1981 final rule was published.\textsuperscript{51} Furthermore, HHS has not shared with IRBs or researchers how it views the notion of privacy in light of the ways that researchers are using the Internet to facilitate their research, and more specifically, have not indicated whether data mining on social networking sites is human subjects research.\textsuperscript{52}

As a result of the changing nature of human subjects research, HHS should again consider whether its definition of a human subject is adequate to ensure the protection of the individuals who enroll in research, whether biomedical, social, or behavioral. In particular, HHS should consider whether clarifications regarding what constitutes private information would better protect human subjects and help researchers and IRBs understand to what type of research these regulations are in fact applicable; that is, when researchers are in fact obtaining identifiable private information.

\begin{itemize}
\item \textsuperscript{47} Id.
\item \textsuperscript{48} See 45 C.F.R. § 46.102(f).
\item \textsuperscript{49} Final Regulations Amending Basic HHS Policy for the Protection of Human Research Subjects, 46 Fed. Reg. at 8373.
\item \textsuperscript{50} Id. at 8366.
\item \textsuperscript{51} Id.
\item \textsuperscript{52} See generally id.
\end{itemize}
III. RESEARCHERS’ USE OF THE INTERNET AND INDIVIDUALS’ EXPECTATION OF PRIVACY

The technological developments made at the end of the 20th century and beginning of the 21st century have significantly influenced the ways in which human subjects research has changed since the federal regulations governing such research were first promulgated. The Internet in particular has greatly influenced the conduct of biomedical research, as well as research in the social and behavioral sciences. There are three important ways in which the Internet is currently used to facilitate human subjects research: use of online surveys, recruitment of participants for studies through online advertisements, and observation of real-time online behavior of individuals.

A. Ways That the Internet Is Used for Research

Through the use of web sites like SurveyMonkey and REDCap, researchers are now able to administer surveys online to vast numbers of research participants. For example, researchers at the University of Utah sent a survey through SurveyMonkey to directors of burn centers across the United States to analyze the frequency of the use of telemedicine for burn care. University of Kentucky researchers used REDCap Survey to ask orthodontists about the types of retainers they give their patients. The distribution of online surveys such as these is typically considered human subjects research, and therefore requires IRB review.

53. SurveyMonkey is a web site that allows users to create and distribute surveys online. SURVEYMONKEY, www.surveymonkey.com (last visited Aug. 9, 2012). Users can create short surveys for a limited number of respondents free of charge, and can pay monthly fees for the right to create more in-depth, more sophisticated surveys. SurveyMonkey Plans & Pricing, www.surveymonkey.com/pricing (last visited Aug. 9, 2012).

54. REDCap (Research Electronic Data Capture) is “a secure, web-based application designed to support data capture for research studies, providing: 1) an intuitive interface for validated data entry; 2) audit trails for tracking data manipulation and export procedures; 3) automated export procedures for seamless data downloads to common statistical packages; and 4) procedures for importing data from external sources.” REDCap, www.project-redcap.org (last visited Aug. 9, 2012). See also Paul A. Harris, Robert Taylor, Robert Thielke, Jonathon Payne, Nathaniel Gonzalez, Jose G. Conde, Research Electronic Data Capture (REDCap) - A Metadata-Driven Methodology and Workflow Process for Providing Translational Research Informatics Support, 42 J. BIOMED. INFORM. 377 (2009). In addition to providing a data management system, the program also includes a survey feature that allows for the administration of online surveys.


57. The distribution of a survey for academic research purposes is human subjects research as long as the project satisfies the regulatory definition of “research,” which is “a systematic investigation, including research development, testing and evaluation, designed to develop or contribute to generalizable knowledge.” 45 C.F.R. § 46.102(d) (2012). The researchers at the University of Utah stated that their study was approved by the IRB. Holt et al., supra note 55, at
Additionally, web sites are often used to advertise studies to recruit potential participants. Pharmaceutical company web sites often include information about the clinical trials they are sponsoring, and even give potential participants the opportunity to do a basic assessment of whether or not they may be eligible to participate in a particular clinical trial.\(^{58}\) Some researchers post advertisements on sites like Craigslist, including information about the study and how to contact the researchers if individuals may be interested in participating.\(^{59}\) In 2000, the U.S. National Institutes of Health (NIH) established a web site called ClinicalTrials.gov that makes a list of clinical trials being conducted in the United States publicly available, and also includes the results of clinical trials that have since closed.\(^{60}\)

The advertisements placed on web sites like Craigslist are included with researchers’ IRB submissions, and are reviewed along with the protocol (description of study procedures, including method for data collection, recruitment and consent processes, and other applicable information), consent documents, and other written materials.\(^{61}\) An IRB’s review of such materials is justified because recruitment represents the beginning of the informed consent process,\(^ {62}\) which is regulated under 45 C.F.R. § 46.116. Furthermore, the OHRP published guidance in 2005 that stated that “[w]hen information posted on a clinical trial website goes beyond directory listings with basic descriptive information, such information is considered part of the informed consent process and therefore requires IRB review and approval.”\(^ {63}\)

Researchers also use the Internet to observe real-time behavior, for example by entering chat rooms and observing the interactions between the site users, and possibly taking part in the interactions themselves. Wake Forest University researchers recently conducted an IRB-approved study in which members of the

---


\(^{59}\) CRAIGSLIST, www.craigslist.com (last visited Aug. 9, 2012). Craigslist postings expire after a short period of time and links to specific advertisements become broken; however, Craigslist advertisements for research participants are often found in a city’s community section, under “volunteers.” See, e.g., http://boston.craigslist.org/vol/.


\(^{61}\) 45 C.F.R. §46.111.


research team entered chat rooms for men who have sex with men. The study methods included interactions with the chat room visitors and the online administration of surveys to willing respondents. The research team disclosed the purpose of its presence in the chat room and sought consent for the online surveys.

These are just three key ways in which the Internet is used in human subjects research. This article, however, focuses on researchers’ use of social networking sites, although some of these uses do not include research with human subjects subject to regulation under 45 C.F.R. § 46.

B. Uses of Social Networking Sites in Research

The purpose of a social networking site is to make individuals available to be contacted and able to contact others for any number of purposes. These sites, which include commonly known sites such as Facebook, MySpace, and Twitter, allow people to post information about themselves, communicate with friends and family, and partake in other activities online, such as playing games. Admissions committees and employers regularly review social networking sites to determine whether a candidate may be suitable for an academic program or job, whether or not the applicant even knows about or has given permission for such a review. The information posted on a social networking site could also prevent a state bar applicant from being admitted to practice law.

---

64. Scott D. Rhodes et al., A Pilot Intervention Utilizing Internet Chat Rooms to Prevent HIV Risk Behaviors Among Men Who Have Sex with Men, 125 PUB. HEALTH REPORTS 29 (2010) (Supp. 1).
65. Id.
66. Id. at 31.
67. Other uses might include re-contacting participants after a study in which they participated months or years before to participate in a new study, or attempting to contact study participants who may be lost to follow-up.
72. Powell, supra note 23, at 163; Gelman, supra note 68, at 1326-27.
Social networking site use among the general public is widespread. Facebook reports having over 900 million users, though the number of unique, active users may be lower. In March 2012, Twitter reported having over 140 million users. Researchers are also using social networking sites more frequently as a means of facilitating their research. For example, in addition to using sites like Craigslist to seek study participants, researchers are turning to sites like Facebook to recruit participants for their studies. Researchers also may use social networking sites to locate and contact participants whose progress they were following after an intervention but fell out of touch with the research team.

In addition to these uses of social networking sites, academic researchers are also more frequently engaging in the practice of data mining on social networking sites as a means of collecting data for biomedical, social, and behavioral research. Often, this is their sole method for data collection in a study. For example, in 2011 researchers at the University of Florida mined the Facebook pages of hundreds of medical students and residents at the university to determine how many of the students and residents posted information that might represent a violation of a patient’s privacy. They ultimately concluded that there had been “significant and increasing evidence of potential privacy violations” that consisted of mostly medical students, but also residents, posting pictures of themselves with patients who could have been identified from the photographs.

The researchers did not specifically request access to anyone’s Facebook page in order to collect the data. Rather, the sole method of data collection was through data mining. The publication reporting the data notes that the researchers accessed the Facebook pages of the medical students and residents via their personal Facebook accounts, viewing the entirety of the publicly
available pages, and only viewing the main photograph and home page of those for which privacy settings had been activated.84

Researchers at Cornell University reviewed the tweets, messages posted on Twitter, of more than two million people to make conclusions about what time of day people are the happiest.85 They concluded, perhaps not surprisingly, that people are in the best mood in the morning, and on weekends.86

Whether this type of research is considered research with human subjects and therefore requires IRB review hinges on whether or not the research involves “human subjects” as defined in 45 C.F.R. § 46.102(f). According to this provision, a “human subject” is “a living individual about whom an investigator (whether professional or student) conducting research obtains (1)[d]ata through intervention or interaction with the individual, or (2)[i]dentifiable private information.”87 I have previously contended that such research is likely not research with human subjects because it does not involve intervention or interaction with any individual and, more importantly for the purposes of this article, does not involve obtaining private information about a person.88

Without any input from HHS on this issue, researchers like those at the University of Florida and Cornell University are left to determine for themselves, or must determine in conjunction with their IRB, whether IRB approval is required in order to conduct their research. If no approval is required, these researchers need not spend the time to put together an IRB application, and the IRB need not spend its limited resources reviewing that which by regulation is not within its purview. Furthermore, if no IRB approval is required, the question of whether researchers may need to obtain informed consent from each individual whose data are mined becomes a contractual issue based on the terms of use of the social networking site, as well as an ethical issue.

IV. PRIVACY, SOCIAL NETWORKING SITES, AND THE LAW

While this article contends that data mining on social networking sites is not human subjects research, it acknowledges that the reason that there is even a question as to whether such research is research with human subjects is because of the lack of clarity about what “private information” really means in today’s society, and, in particular, how the law regards reasonable expectations of privacy today. An in-depth analysis of recent case law supports the contention

84. Id.
86. Id. at 1878.
87. 45 C.F.R. 46.102(f).
88. Solberg, supra note 16, at 321, 324, 328. However, the University of Florida Facebook study was submitted to the institution’s IRB and deemed exempt. Thompson, supra note 80. The Cornell University researchers did not report whether or not their study was submitted to their IRB. See Golder & Macy, supra note 85.
that data mining on social networking sites is not human subjects research because individuals do not have a reasonable expectation of privacy with respect to the information they post on these sites.89

A. Courts Hold No Reasonable Expectation of Privacy on Social Networking Sites

The federal regulations that govern research with human subjects define private information as “information about behavior that occurs in a context in which an individual can reasonably expect that no observation or recording is taking place, and information which has been provided for specific purposes by an individual and which the individual can reasonably expect will not be made public (for example, a medical record).”90 Unfortunately, these regulations do not identify any specific contexts in which individuals may have a reasonable expectation of privacy, and only provide the example of a medical record as information that an individual can reasonably expect will remain private.91 Furthermore, the OHRP has not published any guidance or provided any other advice that identifies such contexts or information.

However, in the last few years, courts have been asked to decide in civil cases whether individuals have a reasonable expectation of privacy in information that they post on social networking sites.92 The opinions provide an excellent means of interpreting the way in which “private information” may be contemplated in 45 C.F.R. § 46 in light of the technology currently available and the way the Internet is being used to conduct academic research.93 Ultimately, courts across the United States are consistently holding that there is no expectation of privacy with respect to the information that people post on social networking sites and have compelled production of this information in a variety of cases.94

The approach that these courts have taken – that sharing information on a social networking site, even with only a small group of people, results in an unreasonable expectation of privacy with respect to the information posted – is one that makes sense when viewed in the context of the privileges that the law

90. 45 C.F.R. § 46.102(f).
91. Id.
92. See, e.g., Jaffee v. Redmond, 518 U.S. 1; Trammel v. United States, 445 U.S. 40; Romano v. Steelcase, 907 N.Y.S. 2d 650. Standards and issues relevant to privacy in criminal cases differ significantly from those applicable to the academic research context. However, the standards and issues present in civil cases represent a better mechanism for exploring expectations of privacy online and in academic research. Thus, this article explores civil, rather than criminal, cases.
93. Id.
typically recognizes.95 A privilege is “an evidentiary rule that gives a witness the option to not disclose the fact asked for, even though it might be relevant; the right to prevent disclosure of certain information in court, especially when the information was originally communicated in a professional or confidential relationship.”96

It is within the context of privilege that I analyze the meaning of “private information” as used in 45 C.F.R. § 46.102(f). The meaning of private information in 45 C.F.R. § 46 is analogous to the meaning of privilege in the rules of evidence.97 The Federal Rules of Evidence recognize that there are certain communications between individuals that are privileged.98 For example, communications between an attorney and client,99 psychotherapist and patient,100 and husband and wife101 may be protected from compelled disclosure. Furthermore, state statutes also may address privileged communications. Tennessee protects communications between, among others, attorney and client,102 social worker and patient,103 psychiatrist and patient,104 husband and wife,105 and accountant and client.106 Any information communicated to individuals under circumstances other than those outlined in these statutes is not protected by the statutory privilege and is subject to disclosure.107

A closer look at these recent cases provides greater insight into how courts view the possibility that privileged information can be posted online, and how these views can help researchers and IRBs determine whether research involves the collection of private information as contemplated in 45 C.F.R. § 46. These cases furthermore provide insight into why information posted on social networking sites is not “information about behavior that occurs in a context in which an individual can reasonably expect that no observation or recording is taking place,” as private information is also defined in 45 C.F.R. § 46.102(f).

In Romano v. Steelcase, the defendant in a personal injury case sought access to the plaintiff’s MySpace and Facebook accounts in an effort to dispute the plaintiff’s claims of injury and loss of enjoyment of life.108 The plaintiff

---

95. See infra notes 99-106.
96. BLACK’S LAW DICTIONARY 1215 (7th ed. 1999).
97. Compare 45 C.F.R. § 46.102(f) (“Private information includes . . . information which has been provided for specific purposes by an individual and which the individual can reasonably expect will not be made public (for example, a medical record”) with BLACK’S LAW DICTIONARY, supra note 96, at 1215.
98. FED. R. EVID. 501.
105. TENN. CODE ANN. §24-1-201 (2011).
asserted her right to privacy regarding her social networking site postings, and thus argued that she should not be required to produce the information from her accounts (including old, deleted postings).\textsuperscript{109} The court held that, “notwithstanding her privacy settings,”\textsuperscript{110} the plaintiff consented to sharing the information that she posted on these sites, as the primary purpose of social networking sites is to share information with others.\textsuperscript{111} The court would therefore not allow her to claim an expectation of privacy with respect to information that was intentionally shared with non-privileged individuals.\textsuperscript{112} It furthermore cited other civil cases in which courts have similarly held that people do not have reasonable expectations of privacy with respect to social networking site postings that they have shared with others,\textsuperscript{113} and, therefore, the court concluded that no expectation of privacy existed in that case.

One of the cases the court cited was \textit{Beye v. Horizon Blue Cross Blue Shield of New Jersey}, a case alleging breach of contract by an insurance company, in which the court ordered the plaintiffs to produce Facebook and MySpace postings discussing their eating disorders because these postings were shared, rather than kept private (like diary entries).\textsuperscript{114} The court ordered this discovery despite the fact that the postings addressed sensitive information about the plaintiffs.\textsuperscript{115} Thus, one can compare \textit{Beye} to a situation where a researcher intends to mine sensitive data from a site like Facebook or MySpace, perhaps about health issues such as eating disorders, and conclude that despite the sensitive nature of the information posted, it is not private information as defined in 45 C.F.R \S 46.

A New York court cited \textit{Romano} in another personal injury case, holding that Facebook postings, if relevant, are still subject to discovery even though privacy settings prevented the general public from accessing the postings.\textsuperscript{116} Likewise, in Pennsylvania, the court in \textit{Largent v. Reed} held that “there is no reasonable expectation of privacy in material posted on Facebook.”\textsuperscript{117} This was also a personal injury case, with the plaintiffs in \textit{Largent} alleging physical injury and pain and suffering as the result of an automobile accident.\textsuperscript{118} The defendant sought access to one plaintiff’s Facebook page because he believed it would reveal photos of the plaintiff at the gym after the accident, thus showing her

\begin{itemize}
\item \textsuperscript{109} \textit{Id.} at 651, 655.
\item \textsuperscript{110} \textit{Id.} at 657.
\item \textsuperscript{111} \textit{Id.}
\item \textsuperscript{112} \textit{Id.}
\item \textsuperscript{113} \textit{Id.} at 656 (quoting Beye v. Horizon Blue Cross Blue Shield of New Jersey, No. 06-5337, 2007 U.S. Dist. LEXIS 100915 (D.N.J. December 14, 2007) (“The privacy concerns are far less where the beneficiary herself chose to disclose the information.”).
\item \textsuperscript{114} Beye, 2007 U.S. Dist. LEXIS 100915, at *9 n3.
\item \textsuperscript{115} \textit{Id.}
\item \textsuperscript{117} Largent v. Reed, No. 2009-1823, at *9 (Pa. C.P. Franklin Co. Nov. 7, 2011).
\item \textsuperscript{118} \textit{Id.} at *2.
\end{itemize}
claims of injury to be without merit.\textsuperscript{119} The court held that “no general privacy privilege protects [plaintiff’s] Facebook material from discovery”\textsuperscript{120} and that she has no reasonable expectation of privacy protecting her Facebook page because “[a]lmost all information on Facebook is shared with third parties, and there is no reasonable privacy expectation in such information.”\textsuperscript{121}

In 2010, in \textit{McMillen v. Hummingbird Speedway}, another Pennsylvania court also refused to recognize any kind of social networking site privilege.\textsuperscript{122} The case was a personal injury case arising from a stock car accident, in which the defendant sought during discovery to obtain log-in information for the plaintiff’s Facebook account to examine whether the extent of the plaintiff’s injuries were as serious as he claimed.\textsuperscript{123} The court opined that, particularly in light of the privacy policies and terms of use that sites like Facebook and MySpace have,\textsuperscript{124} “while it is conceivable that a person could use [social networking sites] as forums to divulge and seek advice on personal and private matters, it would be unrealistic to expect that such disclosures would be considered confidential.”\textsuperscript{125} This court concluded that because “[t]he law does not even protect otherwise privileged communications made in the presence of third parties,”\textsuperscript{126} communications made between non-privileged individuals are “wholly incommensurate with a claim of confidentiality.”\textsuperscript{127}

A third Pennsylvania court following \textit{McMillen} also held that there is no reasonable expectation of privacy in social networking site postings.\textsuperscript{128} The plaintiff in \textit{Zimmerman v. Weis Markets} was an employee of the defendant company when he injured himself.\textsuperscript{129} Although he alleged serious injury, the defendant saw information and photographs posted on public areas of the plaintiff’s Facebook page that indicated that his injuries were not so serious, and accordingly sought access to additional material not shared with the general public.\textsuperscript{130} The court held that because no privilege exists that protects the privacy of the information, and the purpose of a social networking site is to share information with others, no reasonable expectation of privacy exists with respect to the information that is posted.\textsuperscript{131} Furthermore, those with whom the

\textsuperscript{119.} Id. at *5-6.
\textsuperscript{120.} Id. at *9.
\textsuperscript{121.} Id.
\textsuperscript{123.} Id. at *1, 6
\textsuperscript{124.} Id. at *3-4.
\textsuperscript{125.} Id. at *3.
\textsuperscript{126.} Id. at *5.
\textsuperscript{127.} Id.
\textsuperscript{129.} Id. at *1.
\textsuperscript{130.} Id. at *2.
\textsuperscript{131.} Id. at *4, 6.
information is shared are not restricted in terms of how they may in turn share the posted information.132

These opinions support the notion that “private information,” as the term is used in 45 C.F.R. § 46.102(f), does not include information posted by individuals on social networking site pages, and that research involving data mining on social networking sites therefore need not be subject to IRB review because the researchers are not obtaining identifiable, private information about individuals.133 However, these cases are not the only ones that support the contention that mining data on social networking sites is not human subjects research.

In a child custody case, an Ohio court refused to recognize a woman’s right to privacy regarding her MySpace and other blog postings about illegal drug use when it considered whether the trial court erred in considering this evidence when it awarded custody to her daughter’s father.134 It should be noted that this mother told the court that any member of the public could read these postings, and the court accordingly concluded that she could not assert a right to privacy with respect to them.135

Of course, if such blog postings were to be used for research purposes – rather than as evidence in a child custody case, which is what the court was hearing – there are ethical considerations that the researcher should need to take into account at the time of publication. For example, the researcher should consider whether publication of information in a particular way, e.g., by directly quoting the blog post, could lead to the identification of the blog writer. This is especially true when blog posts – such as the ones in this case – discuss engaging in illegal acts.136 Furthermore, the same analysis holds if the information does not reveal illegal behavior but instead pertains to someone’s health condition.137 If a researcher has information about someone and the person could be identified based on the way the information is presented in the publication, even if no individual names are ultimately included in that publication, a researcher should consider the potential consequences that may result of the identification. However, the ethical issues associated with the possible identification of a data source do not necessarily lead to the conclusion that the research is human subjects research and requires IRB review.

In Moreno v. Hanford Sentinel, a California court similarly held that people have no reasonable expectation of privacy with respect to information posted

132. Id. at *8.
133. See supra text accompanying note 88.
135. Id. at *6, n4.
136. See id.
publicly on the Internet. A woman wrote an article about the town in which she grew up. In the article, she included various unfavorable statements about the town and the people who lived there. She then posted it on her MySpace page, and it was available for public viewing, i.e., without any specific access to her page or passwords required. A school principal from the town sent it to the local newspaper before the woman had removed it from her page, and the newspaper later published it, citing her as the author. The woman sued the principal and the newspaper for invasion of privacy and the intentional infliction of emotional distress.

The court held that by posting the article on her MySpace page, the plaintiff “made her article available to any person with a computer and thus opened it to the public eye. Under these circumstances, no reasonable person would have had an expectation of privacy regarding the published material.”

The court further opined that “the fact that [the plaintiff] expected a limited audience does not change [this] analysis.” Thus, blog postings that can be read by anyone with Internet access should not be considered private, even if the writer expects that only a small number of individuals will view the blog. Furthermore, the court stated that the fact that the posting was online for less than a week before it was removed was irrelevant and held that the posting “was not so obscure or transient that it was not accessed by others.” Thus, if a researcher collected information from blog posts that had only been posted a short amount of time and were removed fairly soon after being posted, the author may have a difficult time justifying a reasonable expectation of privacy simply because they were posted only for a brief period of time.

These decisions are helpful in evaluating the issue of whether researchers who mine and analyze information posted on social networking sites need to submit their research to their IRBs for review and approval. The cases can be applied to analyze, for example, the question that Internet research ethics scholar Elizabeth Buchanan posed in her presentation about Internet research in the Summer of 2010 to the Secretary’s Advisory Committee on Human Research Protections. In this presentation, she asked whether a researcher who analyzes

139. Id. at 1128.
140. Id. at 1128, 1130.
141. Id. at 1128.
142. Id. at 1129.
143. Id. at 1130.
144. Id.
145. Gelman, supra note 68, at 1341.
147. See id.
blog postings must submit the study for IRB review or risk the inability to publish the work.\textsuperscript{149} The analysis that can be used to answer this question is no different from the analysis that can be used to determine whether individuals who post on Facebook or Twitter have a reasonable expectation of privacy, and the essential part of this analysis again is whether the information contained in the blog posts to be analyzed is private.\textsuperscript{150} It would therefore appear that Professor Buchanan’s question can be answered using the same analysis that the courts have used to answer the question of whether information posted on social networking sites is private.

\textbf{B. Reasonable Expectations of Privacy: Counter-Arguments}

The fact that courts are recognizing that sharing information with even a limited number of third parties reduces or eliminates any reasonable expectation of privacy that an individual can have with respect to information they post on a social networking site means that it is reasonable to interpret “private information” as described in 45 C.F.R. § 46 to exclude information posted on a social networking site. However, the argument has been posited that people who post on social networking sites may have some reasonable expectation of privacy with respect to the posted information if they limit the number of people who may access the information, \textit{e.g.}, by adjusting the privacy settings on their accounts.\textsuperscript{151}

Internet scholar Michael Zimmer, for example, addressed this argument in an article where he criticizes the way in which a data set that Harvard University researchers created based on information posted on the Facebook pages of the students in Harvard’s class of 2009 was published.\textsuperscript{152} These researchers, who created the data set to make it available to other researchers, claimed that the data had been de-identified, and Professor Zimmer explains how easily the individuals whose information had been mined and recorded could be re-identified.\textsuperscript{153}

Professor Zimmer was furthermore concerned about the way in which data was collected from the individual Facebook pages to compile this data set due to the expectations of privacy that those whose information was recorded may have had with respect to their Facebook pages.\textsuperscript{154} The Harvard researchers were able

\addcontentsline{toc}{section}{Notes and References}

\footnotesize
\bibitem{149}Id.
\bibitem{150}In accordance with federal regulations, the information must also be identifiable, but for purposes of this analysis, I am presuming that the information is identifiable and therefore the only remaining issue is whether it is private. The ability or inability to identify an individual who posts information online is outside of the scope of this article.
\bibitem{151}See, \textit{e.g.}, Michael Zimmer, “\textit{But the data is already public}”:\textit{ On the Ethics of Research in Facebook}, 12 ETHICS INFO. TECH. 313, 318 (2010) (discussing Kevin Lewis et al., \textit{Tastes, Ties, and Time: A New Social Network Dataset Using Facebook.com}, 30 SOCIAL NETWORKS 330 (2008)).
\bibitem{152}See generally id.
\bibitem{153}Id. at 316-17.
\bibitem{154}Id. at 318.
to mine the Facebook data with the help of research assistants who otherwise had access to the individual Facebook pages, likely because they were all part of the same network(s). Professor Zimmer argues that because some individuals may have adjusted their privacy settings to only allow certain individuals to access their Facebook pages, the fact that the research assistants were part of a group that was given limited access does not mean that these individuals intended for their information to then be used by the research assistants for research purposes. He further contends that such use “puts the privacy of those subjects at risk.”

Other scholars have similarly contended that “a regime that fails to recognize that not everything posted on the Internet is meant for every user of the Internet, fails to understand the technology and its potential.”

One court may agree. Although Moreno held that there is no expectation of privacy in information posted on the Internet that is available to the general public, the court nevertheless conceded that, “information disclosed to a few people may remain private.” This statement supports arguments like Professor Zimmer’s that those who limit access to their Facebook page to a small group of Friends, for example, have a reasonable expectation of privacy with respect to that information because they activated their privacy settings to restrict access to only a select group of people (rather than making their page completely public). However, the Moreno court appears to be the exception with respect to that analysis, as both Largent and Romano held that disclosure of information to any third parties—even if only to a small group—on a social networking site is enough to destroy any reasonable expectation of privacy with respect to that information.

The Stored Communications Act has also been argued as a reason that individuals have a reasonable expectation of privacy in postings on social networking sites. The Act prohibits companies like Facebook and MySpace from being compelled to produce information in civil cases such as private email and instant messages that were exchanged between site users through the sites, as both Facebook and MySpace provide electronic communication services and remote computing services. Such a prohibition has led parties to argue that

155. Id.  
156. Id. (“While the information was indeed available to the R[esearch] A[ssistant], it might have been accessible only due to the fact that the RA was within the same ‘network’ as the subject, and that a privacy setting was explicitly set with the intent to keep that data within the boundaries of that network.”)  
157. Id.  
158. Gelman, supra note 68, at 1344.  
161. See Zimmer, supra note 151.  
they have a reasonable expectation of privacy in postings they have made on Facebook, as well as a reasonable expectation of privacy with respect to private messages exchanged between Facebook or MySpace users, since the companies are prohibited by federal law from disclosing the exchanges. However, it should be emphasized that the Stored Communications Act only applies to entities that are providers of electronic communication services or remote computing services.

Interestingly, the court in Crispin v. Christian Audigier, Inc. held that there was not enough evidence for it to decide whether or not the Facebook wall messages and MySpace comments could be compelled, but any decision by the court that these comments could be compelled may affect the analysis of whether data mining on social networking sites by academic researchers is human subjects research.

I contend that sharing information with even a select group of people on a social networking site reduces the expectation of privacy that one can have with respect to that information, and as a result, researchers who mine data on social networking sites are not conducting research with human subjects. However, my disagreement does not mean that the ethical conduct of the research is unimportant. It is important that basic principles of research ethics guide researchers so that they respect the privacy of the individuals whose data they are mining (even if what they are mining is not “private information”). However, whether or not there are ethical concerns is an issue separate and apart from whether IRB review is required.

V. A NEW KIND OF SOCIAL NETWORKING SITE

Although this article has discussed several publications whose authors analyzed data collected from social networking site postings, not all social networking sites fit the mold of Facebook, MySpace, and Twitter. Thus, the changing nature of social networking sites provides a persuasive reason for HHS to carefully consider whether data mining on social networking sites is human subjects research. The conclusion that data mining on sites like these to conduct academic research is based in part on the premise that the purpose of a social networking site is to share information with others, but also on the premise that social networking sites like these allow almost anyone to register and create

166. See Crispin, 717 F. Supp. 2d at 991.
167. See Stored Communications Act § 2702.
169. See supra text accompanying note 136-37 (describing the importance of conducting research ethically even though it may not be human subjects research).
170. See Zimmer, supra note 151, at 324 (“[I]t is our responsibility [ ] to ensure our research methods and processes remain rooted in long-standing ethical practices.”)
171. See, e.g., Golder & Macy, supra note 85; Thompson, supra note 80.
172. Gelman, supra note 68, at 1326.
an account where they can post information for others to view. There is, however, a new social networking site that is increasing in popularity that forces a more nuanced approach to determining whether data mining on social networking sites is human subjects research subject to regulation under 45 C.F.R. §46.

Founded in 2004, PatientsLikeMe provides users with more than just a general social networking opportunity, and is indeed more restrictive regarding who may become a user than Facebook, MySpace, or Twitter, although it has been described as appearing “[a]t first glance...like just any other online community, a kind of MySpace for the afflicted.” Now with more than 150,000 users, PatientsLikeMe was designed to provide patients with the tools to create a profile where they can record information about their health, analyze their own health data, and then compare it to others. Although data mining on this type of website will not serve as a complete substitute for traditional Phase I-IV clinical trials, academic researchers can gather important data from patients who post information about themselves and their health care online.

Given the public’s widespread use of the Internet to learn more about their health and health care, it is unsurprising that a health care-specific social networking site has been developed, particularly given the popularity of sites like WebMD that people turn to regularly (for better or for worse) for information about their health. The abundance of articles that the PatientsLikeMe employees/researchers have published to date based on data collected from participants on the site (whether through data mining or surveys) clearly

173. Facebook, for example, allows anyone over the age of 13 to register for a Facebook account. Statement of Rights and Responsibilities, FACEBOOK, http://www.facebook.com/legal/terms?ref=pf (last visited Aug. 9, 2012). Twitter requires that its users be able to “form a binding contract with Twitter” and prohibits use of the site by anyone who by law has been banned from using it. Terms of Service, TWITTER, http://twitter.com/tos (last visited Aug. 9, 2012). In the United States, this effectively means that almost everyone over the age of 18 can register for a Twitter account.


176. PATIENTSLIKEME, supra note 174.

177. Gerald C. Kane et al., Community Relations 2.0, Harv. Bus. Rev., Nov. 2009, at 45, 46 (“Patients volunteer details about their diseases and the treatments they’ve pursued – including those not prescribed by their doctors. Charts and progress curves on the website help people to visualize their own complex treatment histories, allow comparisons among peer groups, and prompt members to provide feedback and advice on one another’s progress.”); id.


179. Kane, supra note 177, at 46 (“A report from Manhattan Research suggests that more than 60 million Americans are consumers of ‘health 2.0’ resources. They read or contribute to blogs, wikis, social networks, and other peer-produced efforts, using Google as the de facto starting point.”).

180. The New York Times has referred to WebMD as an “enormous and powerful site” that is also a “hypochondria time suck.” Virginia Heffernan, A Prescription for Fear, N.Y. TIMES, Feb. 4, 2011, at MM14.
indicates that this is a resource ripe for mining by other researchers.\textsuperscript{181} In 2011, for example, the researchers mined data from the site about patients who reported taking two particular drugs for an off-label purpose (\textit{i.e.}, a use not approved by the FDA), and published an article with their conclusions about the frequency and types of off-label uses and the reported side effects of these medications.\textsuperscript{182}

What is unclear, however, is whether mining sites like PatientsLikeMe should be treated like mining Facebook (and therefore is not human subjects research) or if data mining on a site like PatientsLikeMe requires that a different conclusion be reached. It is the unique nature of PatientsLikeMe that forces this question, which depends on whether the expectations of privacy of PatientsLikeMe users differ from – or perhaps more important, should differ from – the expectations of privacy of Facebook or MySpace users.

PatientsLikeMe, unlike Facebook or MySpace, requires users to certify that they are members of one or more groups, such as a person with a particular disease, or a caregiver of a person with a particular disease, in order to register.\textsuperscript{183} A health care professional, including one who is a “health researcher,” is also permitted to register on the site.\textsuperscript{184} However, the site’s User Agreement lacks provisions addressing what uses a health researcher could make of the information posted on site users’ profiles.\textsuperscript{185} The User Agreement only prohibits the use of the site for “commercial purposes,” prohibiting “organizations, companies, and/or businesses,” as well as “representatives from life sciences and insurance companies” from becoming members, using the site, or creating profiles.\textsuperscript{186} No definition of “commercial purposes” is provided, but a biomedical researcher employed at a university who mines data on PatientsLikeMe solely for the purpose of preparing an academic publication is likely not using the site for commercial purposes, \textit{i.e.}, to make money. Furthermore, on the site’s R&D policy, which is simply a list of FAQs about conducting research using the site, PatientsLikeMe separates questions about

\textsuperscript{181} A February 2012 search on PubMed for articles that included the term “PatientsLikeMe” yielded nineteen articles, fifteen of which included at least one author who is an employee of PatientsLikeMe. Of the four remaining articles, only one mined data on PatientsLikeMe to assess the medical terminology used, with a goal of augmenting an online health vocabulary application. See Kristina Doing-Harris & Qing Zeng-Treitler, Computer-assisted update of a consumer health vocabulary through mining of social network data, 13 J. MED. INTERNET RES. e13 (2011).

\textsuperscript{182} Jeana Frost et al., Patient-reported Outcomes as a Source of Evidence in Off-Label Prescribing: Analysis of Data from PatientsLikeMe, 13 J. MED. INTERNET RES. e6 (2011). The authors of the article are employees of PatientsLikeMe, and not from an academic institution.

\textsuperscript{183} User Agreement, PATIENTSLIKEME, http://www.patientslikeme.com/about/user_agreement (last visited Aug. 9, 2012).

\textsuperscript{184} Id.

\textsuperscript{185} Id.

\textsuperscript{186} Id.
“commercial research” from questions about “non-commercial/academic
research.”

Thus, one can conclude that the User Agreement does not anticipate that
academic researchers are using the site for commercial purposes, and that the use
of PatientsLikeMe for academic research purposes is therefore permissible
without explicit permission from the site. If explicit permission from
PatientsLikeMe is not required for academic researchers to mine the site for
research purposes, PatientsLikeMe users arguably have a lower expectation of
privacy with respect to the information they post on the site than they would if
explicit permission were required. This is because if explicit permission were
required, the pool of individuals who could mine their information would likely
be smaller than the pool who may mine their information when such permission
is not required.

The research published by PatientsLikeMe employees also provides some
insight into the expectations of the site users with respect to research. In an
article about multiple sclerosis patients and their barriers to adhering to their
medication regimens which reported the results of surveys completed by
registered PatientsLikeMe site users, the authors state that “[m]embers of
PatientsLikeMe join the site with the expectation that they will be participating
in research.” The authors do not take this statement one step further to clarify
whether this means that individuals who join PatientsLikeMe expect that they
will be asked to participate in surveys, or if individuals who join expect that the
information they post will be used for research purposes, or both. However, if
PatientsLikeMe users are joining with the expectation that, in general, they will
be research participants by virtue of their membership on the site, they again

187. PatientsLikeMe, Frequently Asked Questions about research at PatientsLikeMe,
visited Aug. 9, 2012).

188. Unfortunately, PatientsLikeMe does not state its policy on what types of approval are
required from the site to conduct independent academic research; instead, it only comments on
academic research done in collaboration with PatientsLikeMe. Id. By way of comparison,
Facebook’s Statement of Rights and Responsibilities provides that “If you collect information from
users, you will: obtain their consent, make it clear you (and not Facebook) are the one collecting
their information, and post a privacy policy explaining what information you collect and how you
will use it.” Statement of Rights and Responsibilities, FACEBOOK, http://www.facebook.com/
legal/terms (last visited Aug. 9, 2012). However, much like on PatientsLikeMe, an ambiguity likely
exists for individual users about the meaning of this provision. Facebook does not define the term
“collect” and there are certainly a number of uses that are made of Facebook for which consent of
individuals is not sought but their information may be considered “collected.” See supra notes 73-
74. Thus, it is unlikely that a Facebook user could claim a reasonable expectation of privacy
regarding information posted on her page because of this provision in the Statement of Rights and
Responsibilities. Should Facebook amend this provision in the future, further investigation about
expectations of privacy of Facebook users may be warranted.

189. Paul Wicks et al., Use of an Online Community to Develop Patient-Reported Outcome
Instruments: The Multiple Sclerosis Treatment Adherence Questionnaire (MS-TAQ), 13 J. MED.
INTERNET RES. e12 (2011).
should have reduced expectations of privacy with respect to the information they post.

It would seem that notions of reasonable expectations of privacy change may when people post information specifically about their health online. Laws like the Health Insurance Portability and Accountability Act (HIPAA) exist to prevent the unauthorized disclosure of an individual’s protected health information by third parties such as doctors, nurses, and insurance companies (what are called, under HIPAA, “covered entities”). However, there are no HIPAA implications with respect to posting information on PatientsLikeMe because the site is not a covered entity. Additionally, “health information stored by a patient on an online health profile – or even a personal filing cabinet – has no claim to privacy.” Therefore, PatientsLikeMe users have an ever further reduced expectation of privacy in the information they post.

It is therefore difficult to say with certainty that data mining on a site like PatientsLikeMe is human subjects research under 45 C.F.R. § 46 because placing restrictions on who can join a site is indicative of a more reasonable expectation of privacy that individuals. However, these restrictions do not eliminate health researchers from joining the site and mining the data on it for research purposes. Furthermore, PatientsLikeMe’s statement that people who join the site expect to be research participants could be viewed as a warning to potential and current site users that use of the site comes with the possible “risk” of being a research participant. Coupled with the argument that individuals cannot expect that health information they disclose to someone other than a covered entity will remain private, a court could determine that despite the stricter registration requirements on a site like PatientsLikeMe, if the User Agreement specifically allows researchers to join the site and consequently have access to all users’ profiles, and if site users join knowing they will be research participants, information posted on the site would not be considered private information. By extension, under 45 C.F.R. § 46, it is unlikely that mining that information would be human subjects research.

191. If PatientsLikeMe was a covered entity, it would be legally obligated to protect the health information shared by its users, but it is not a covered entity because it is not a health care provider. James Grimmelmann, PatientsLikeMe: A Study in Online Community Issues, PRAWFSBLAWG, http://prawfsblawgblogs.com/prawfsblawg/2008/03/the-latest-new.html (Mar. 24, 2008, 9:30 EST).
VI. SUGGESTED LANGUAGE FOR GUIDANCE OR REGULATORY PROVISIONS

HHS understands that the nature of human subjects research has changed since the 1970s, and even since the Common Rule was codified in 1991.\footnote{The 1991 final rule that represents the most recent revision of the Common Rule was published following a 1988 notice of proposed rulemaking that proposed a set of regulations that would apply to research funded by agencies other than just HHS (and would therefore be “common” to these federal agencies, thus resulting in the term “the Common Rule.”). Federal Policy for the Protection of Human Subjects, 53 Fed. Reg. 45660, 45661 (Nov. 10, 1988) (to be codified at 45 C.F.R. pt. 46).} The agency furthermore acknowledges that the Internet in particular has played a major role in the way such research is conducted now as compared to more than twenty years ago.\footnote{Human Subjects Research Protections: Enhancing Protections for Research Subjects and Reducing Burden, Delay, and Ambiguity for Investigators, 76 Fed. Reg. 44512 (July 26, 2011).} In July 2010, a panel was convened at the meeting of the Secretary’s Advisory Committee on Human Research Protections (SACHRP) to inform the SACHRP about how the Internet is used in human subjects research, and how the Internet affects our understanding of the way the regulations now must be applied to proposed research.\footnote{Buchanan, supra note 148. See text accompanying note 148 supra (discussing Professor Buchanan’s presentation to the Secretary’s Advisory Committee on Human Research Protections in July 2010).}

One year later, in July 2011, HHS published an advance notice of proposed rulemaking (ANPRM) in the Federal Register that sought comments “on how to better protect human subjects who are involved in research, while facilitating valuable research and reducing burden, delay, and ambiguity for investigators.”\footnote{Human Subjects Research Protections: Enhancing Protections for Research Subjects and Reducing Burden, Delay, and Ambiguity for Investigators, 76 Fed. Reg. at 44512 (emphasis added).} This was the first time since 1988 that HHS publicly requested comments about significant revisions to 45 C.F.R. § 46.\footnote{Although notices of proposed rulemaking have been published since 1988, none have sought to make the major changes to 45 C.F.R. § 46 that the 1988 notice and 2011 advance notice proposed.} HHS again recognized the changes that the Internet has caused in the way human subjects research is conducted, admitting that

\begin{quote}
[\hspace{1mm}\text{a\hspace{-1mm}l\hspace{-1mm}i\hspace{-1mm}though\hspace{-1mm} the\hspace{-1mm} regulations\hspace{-1mm} have\hspace{-1mm} been\hspace{-1mm} amended\hspace{-1mm} over\hspace{-1mm} the\hspace{-1mm} years,\hspace{-1mm} they\hspace{-1mm} have not\hspace{-1mm} kept\hspace{-1mm} pace\hspace{-1mm} with\hspace{-1mm} the\hspace{-1mm} evolving\hspace{-1mm} human\hspace{-1mm} research\hspace{-1mm} enterprise,\hspace{-1mm} the proliferation of multi-site clinical trials and observational studies, the expansion of health services research, research in the social and behavioral sciences, and research involving databases, the Internet, and biological specimen repositories, and the use of advanced technologies, such as genomics.}]
\end{quote}

\footnote{The 1991 final rule that represents the most recent revision of the Common Rule was published following a 1988 notice of proposed rulemaking that proposed a set of regulations that would apply to research funded by agencies other than just HHS (and would therefore be “common” to these federal agencies, thus resulting in the term “the Common Rule.”). Federal Policy for the Protection of Human Subjects, 53 Fed. Reg. 45660, 45661 (Nov. 10, 1988) (to be codified at 45 C.F.R. pt. 46).}

\footnote{Human Subjects Research Protections: Enhancing Protections for Research Subjects and Reducing Burden, Delay, and Ambiguity for Investigators, 76 Fed. Reg. at 44512 (emphasis added).}
Furthermore, HHS acknowledges that “[t]he advent of sophisticated computer software programs, the Internet, and mobile technology have created new areas of research activity, particularly within the social and behavioral sciences, exponentially increasing the amount of information available to researchers, while providing the means to access and analyze that information.”

It will likely be quite some time before HHS publishes a notice of proposed rulemaking in response to the comments solicited from the ANPRM, but it is possible, based on HHS’s acknowledgements in the ANPRM of the effect the Internet has had on human subjects research, that privacy issues as they relate to the Internet will be addressed. To that end, I am proposing some language that represents what I believe HHS should incorporate into any revisions of 45 C.F.R. § 46, or that the OHRP could incorporate into guidance for researchers and IRBs. This language reflects the changes that the Internet has brought about in human subjects research.

With respect to the use of the Internet to distribute surveys, I propose the following new language:

The distribution of a survey via the Internet may be exempt under 45 C.F.R. § 46.101(b)(2) or 45 C.F.R. § 46.101(b)(3). However, for all non-exempt research, the distribution of a survey via the Internet requires informed consent obtained in accordance with 45 C.F.R. § 46.116(a)-(b) unless the IRB determines that the research satisfies the criteria for a waiver or alteration of informed consent under 45 C.F.R. § 46.116(c) or 45 C.F.R. § 46.116(d).

With respect to the use of the Internet to recruit research participants, HHS could simply add provisions that incorporate the guidance that the OHRP published in 2005 about advertisements on clinical trial web sites. However, this guidance should be expanded to apply not just to web advertisements for clinical trials, but for web (and possibly even paper) advertisements for any type of research with human subjects.

The OHRP has already stated that such advertisements, if they include more than basic information about a trial, are part of the informed consent process and

200. Id. at 44513.

201. One scholar is not so hopeful, however. Professor Alexander Halavais, the President of the Association of Internet Researchers, believes that “[t]he proposed changes should reduce many of the burdens currently imposed on researching open discourse on the web – such as studying blog posts or tweets. It is, however, unlikely to make standards of privacy clearer…” Alexander Halavais, Open Up Online Research, 480 NATURE 174, 175 (2011).


203. The guidance was published because the HHS Office of the Inspector General recommended that the OHRP do so, and the recommendation was made specifically with reference to clinical trial web sites. However, the Internet is used to recruit for more than just clinical trials. See, e.g., Mary Ann Chiasson et al., HIV Behavioral Research Online, 83 J. URBAN HEALTH 73 (2006); Robert Kraut et al., Psychological Research Online, 59 AMER. PSYCHOL. 105, 106 (2004) (identifying web sites where advertisements for research participants may be located).
therefore must be reviewed by the IRB. Furthermore, the OHRP identifies what it considers “basic information.” This guidance provides excellent assistance to IRBs and researchers about what needs to be submitted to the IRB, and what the IRB should consider when it reviews the advertisement. The descriptive information included in the guidance about what IRBs should consider when reviewing these web advertisements – such as the way in which incentives are described – is most appropriately left to guidance. However, HHS’s recognition in the ANPRM of the widespread use of the Internet for research purposes should be taken one step further into the drafting of a new provision that reads as follows, nearly identically to what is currently written in the OHRP guidance:

When information posted on a web site to recruit participants in human subjects research goes beyond directory listings with basic descriptive information, such information is considered part of the informed consent process and therefore requires IRB review and approval. Basic descriptive information includes: study title, purpose of the study, protocol summary, basic eligibility criteria, study site location(s), and how to contact the study site for further information. Information exceeding such basic listing information includes descriptions of study risks and potential benefits, or solicitation of identifiable information. All documents that will be distributed to participants in order to obtain their informed consent must be reviewed by the IRB.

With respect to data mining online, OHRP guidance or HHS regulations should include language similar to the following:

The following activities on the Internet are not human subjects research:

1. Searching for and recording information about individuals that is posted on any website that does not require a password in order to view the site.
2. Searching for and recording information about individuals that is posted on any website if the individual posts the information with the specific designation that it be viewable to the public (for example, a specifically designated public Facebook page).
3. Searching for and recording information about individuals that is posted on any website for which a password is required to enter the website and/or is not otherwise viewable by the general public if the website does not require any certification by the researcher of his purpose for using the website.

204. OHRP, Guidance on Institutional Review Board Review of Clinical Trial Websites, supra note 63.
205. Id. (“Basic descriptive information includes: study title; purpose of the study; protocol summary; basic eligibility criteria; site study location(s), and; how to contact the study site for further information.”)
206. Id.
207. See id. Note again that this language that I am proposing is nearly identical to the language in the current guidance.
4. The use of spyware, software, or other covert technological means such as “hacking” to access information online is not permitted without the permission of the IRB.

VII. CONCLUSION

The Internet is used in many ways to facilitate research, and in particular to facilitate research with human subjects. Based on the current definition of a human subject in 45 C.F.R. § 46, it does not appear that data mining on social networking sites is human subjects research because it involves neither intervention nor interaction with individuals about whom data are obtained. In light of current reasonable expectations of privacy regarding uses of social media, it furthermore does not involve the collection of identifiable, private information about individuals. However, even if data mining on social networking sites is not human subjects research, it is nevertheless important that research facilitated by social media be conducted ethically. At the same time, though, institutions and IRBs must be careful not to conflate the issues of ethical research and research that is subject to regulation under 45 C.F.R. § 46. Simply because research involves the analysis of sensitive personal information does not mean that the research necessarily involves the analysis of identifiable private information.

To reduce the confusion of researchers and IRBs, HHS, as part of its reconsideration of 45 C.F.R. § 46 in its current form, should consider revising the regulations or supplementing them with guidance that addresses the meaning of private information in light of the technological age in which we live. Furthermore, HHS should promulgate regulations that address Internet research, and specifically data mining on sites like social networking sites, or publish guidance to assist researchers and IRBs with understanding when such research is human subjects research and requires IRB review (or at a minimum, a designation of an exemption).