<table>
<thead>
<tr>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Courts in the Drone Age</td>
<td>161</td>
</tr>
<tr>
<td>Reverse Sunshine in the Digital Wild Frontier: Protecting Individual Privacy Against Public Records Requests for Government Databases</td>
<td>191</td>
</tr>
<tr>
<td>The Changing Expectation of Privacy: Keeping Up with the Millennial Generation and Looking Toward the Future</td>
<td>287</td>
</tr>
<tr>
<td>A World Information Order — Privacy and Security in a Hyper-networked World of Data and Analysis</td>
<td>315</td>
</tr>
<tr>
<td>More Data Mining for Medical Misrepresentation? Admissibility of Statistical Proof Derived from Predictive Methods of Detecting Medical Reimbursement Fraud</td>
<td>341</td>
</tr>
<tr>
<td>COBRA Data and the Right to Confront Technology Against You</td>
<td>375</td>
</tr>
<tr>
<td>The Fiction of Privacy Under the Fourth Amendment: Examining Warrantless Cell Phone Searches in the Context of Riley v. California</td>
<td>395</td>
</tr>
</tbody>
</table>
Special Thanks to
Jeannine Abukhater Lambert

COPYRIGHT © NORTHERN KENTUCKY UNIVERSITY
Cite as 42 N. KY. L. REV. (2015)

Northern Kentucky Law Review is published three times during the academic year by students of Salmon P. Chase College of Law, Northern Kentucky University, Highland Heights, Kentucky 41099. Telephone: 859/572-5444. Facsimile: 859/572-6159. Member, National Conference of Law Reviews. All sections which appear in this issue are indexed by the H.W. Wilson Company in its Index to Legal Periodicals. Northern Kentucky Law Review articles are also available on microfilm and microfiche through University Microfilms International, Ann Arbor, Michigan.

Subscription rates are $35.00 per volume, $10.00 per individual issue. If a subscriber wishes to discontinue a subscription at its expiration, notice to that effect should be sent to the Northern Kentucky Law Review office. Otherwise, it will be assumed that renewal of the subscription is desired.

Please send all manuscripts to the address given above. No manuscript will be returned unless return is specifically requested by the author.
SALMON P. CHASE COLLEGE OF LAW

JEFFREY STANDEN, A.B., J.D.
Dean & Professor of Law

LAWRENCE ROSENTHAL, B.A., J.D., LL.M.
Associate Dean for Academics & Professor of Law

JENNY YOUNG
Registrar of the College of Law

LISA MOORE, B.A., J.D.
Director of Career Services

MICHAEL J.Z. MANNEIMER, B.A., J.D.
Associate Dean for Faculty Development & Professor of Law

ASHLEY GRAY, B.A., J.D.
Director of Admissions

BECKY FITZSIMMONS, B.A., J.D.
Associate Dean for Administration

SHERRIE TURNER, B.S., M.P.A.
Budget Analyst

DAVID H. MACKNIGHT, B.S., J.D.
Associate Dean for Law School Advancement

MICHAEL WHITEMAN, B.A., M.S.L.S., J.D.
Associate Dean for Library Services and Information Technology & Professor of Law

FACULTY

ERIC ALDEN, B.A., M.A., J.D.
Assistant Professor of Law

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.
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.
Professor of Law

HARRY "Hap" DURKIN, B.S.
Director of Development

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

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 & Director of The Lunsford Academy

AMY HALBROOK, B.A., J.D.
Director of Children’s Law Center Clinic & Assistant Professor of Law

JACK HARRISON, B.A., J.D.
Assistant Professor of Law

THOMAS E. HEARD, B.A., M.L.S., J.D.
Associate Professor of Library Services & Associate Director for Library Services

DENNIS HONABACH, A.B., J.D.
Professor of Law

LINDSEY JAEGER, B.A., J.D., S.S.B.B.
Director of Communication

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.
Associate Professor of Legal Writing

JENNIFER KINSLEY, B.A., J.D.
Assistant Professor of Law & Field Placement Program Director

JENNIFER KREDER, B.A., J.D.
Professor of Law

JEANNINE ABUKHATER LAMBERT, B.A., J.D.
Assistant Director of Advancement Centers & Institutes

JENNIFER MART-RICE, B.A., M.S.L.S., J.D.
Assistant Professor of Law & Assistant Director for Collection Development, Serials and Acquisitions

BARBARA MCFARLAND, B.S., J.D.
Assistant Professor of Law & Director of Student Success Initiatives

LIUBOMIR NACEV, B.A., J.D., LL.M.
Professor of Law

DAVID SINGLETON, B.A., J.D.
Assistant Professor of Law & Director of Constitutional Litigation & Indigent Defense Clinics

GERARD ST. AMAND, A.B., J.D., M.S.
Professor of Law

MARK M. STAVSKY, B.A., J.D., LL.M.
Professor of Law

HENRY L. STEPHENS, JR., B.A., J.D.
Professor of Law

JANE UNDERWOOD, B.A., M.L.S., J.D.
Assistant Professor of Law Library Services & Assistant Dean for Students

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

BARBARA WAGNER, B.A., M.S.B.A., J.D.
Assistant Professor of Law & Director of Small Business & Nonprofit Law Clinic

CARYL A. YZENBAARD, A.B., J.D.
Professor of Law
EMERITI FACULTY
WILLIAM R. JONES, B.S., M.A., J.D.

ADJUNCT FACULTY

DONYETTA BAILEY, B.S., J.D.
DAVID BARRON, J.D.
HON. GREGORY M. BARTLETT, A.B., M.A., J.D.
JOHN BENINTENDI, J.D.
VICTORIA BOGGS, B.A., J.D.
NAIMA CLARKE, B.B.A., J.D.
ERIN CORKEN, B.F.A., J.D.
 JOHN CRUZE, B.S., J.D.
PETER DEHAAN, B.S., J.D.
REBECCA DILORETO, B.A., J.D.
ROBERT A. GOERING, JR., B.A., J.D.
ROBERT A. GOERING, SR., B.A., J.D.
WILLIAM GUSTAVSON, B.A., J.D.
SHERYL HEETER, J.D.
PENNY HENDY, J.D.
NANCY HERBERT, J.D.
HON. STEVEN R. JAEGER, B.A., J.D.
DAVID JEFFERIES, B.A., J.D.
RICHARD KATZ, B.A., J.D.
JOHN KROPP, J.D.

JOSEPH MORDINO, J.D.
FRANK MUNGO, B.S., J.D.
DANIEL MURNER, B.A., J.D.
MARC PERA, J.D.
WILLIAM A. POSEY, J.D.
STEVEN RAY, B.A., J.D.
ERIC W. RICHARDSON, B.A., J.D.
DEBRA ROTHSTEIN, B.A., M.A., J.D.
THOMAS ROUSE, J.D.
ANN SCHOEN, B.S., J.D.
HON. DOUGLAS STEPHENS, B.A., 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.
AL WEISBROD, J.D.
ELIZABETH WINCHELL, J.D.
JUSTICE DONALD C. WINTERSHEIMER, A.B., M.A., J.D.
J. STEPHEN WIRTHLIN, JR., B.A., J.D.
ELIZABETH ZINK-PEARSON, J.D.
ARTICLES

Courts in the Drone Age
Timothy M. Ravich .................................................................................................................... 161

Reverse Sunshine in the Digital Wild Frontier: Protecting Individual Privacy Against Public Records Requests for Government Databases
Jennifer A. Brobst ..................................................................................................................... 191

The Changing Expectation of Privacy: Keeping Up with the Millennial Generation and Looking Toward the Future
Erin Corken ..................................................................................................................................... 287

A World Information Order — Privacy and Security in a Hyper-networked World of Data and Analysis
Michael Losavio, Youngjin Song, Joshua I. James, Andrew Marrington, K.P. Chow................................. 315

More Data Mining for Medical Misrepresentation? Admissibility of Statistical Proof Derived from Predictive Methods of Detecting Medical Reimbursement Fraud
Neil Issar ......................................................................................................................................... 341

NOTES

COBRA Data and the Right to Confront Technology Against You
Kathleen E. Watson .......................................................................................................................... 375

The Fiction of Privacy Under the Fourth Amendment: Examining Warrantless Cell Phone Searches in the Context of Riley v. California
Casey A. Taylor ............................................................................................................................. 395
Courts in the Drone Age

Timothy M. Ravich

Abstract

Within the “Internet of Things,” few contemporary subjects more than “drones” encapsulate “informatics,” loosely defined as the study of the application of computer technology to manage information and knowledge in business, legal, and social processes (think Facebook, political polling, and medical records storage). Aviation—from free-floating balloons to orchestrated jet operations—is nothing new in public, military, and private settings, but the use of unmanned aerial vehicles (“UAVs”) for civil, commercial, educational, law enforcement, and national security purposes is novel. This is not because UAV technology necessarily offers anything groundbreaking in the way of aeronautics; rather, UAVs are transformational information collection, storage, and management systems in terms of digital forensics. The range of intelligence, surveillance, and reconnaissance (“ISR”) capabilities made possible by sensor suites and software solutions deployed on UAV platforms seems limitless. This boundless use extends to legal processes, where the job of litigants and triers of fact could be eased and optimized through the use of drone-acquired evidence, for example high-definition video of accident or crime scenes.

But, what if a drone uses facial recognition or other biometric matching technology to acquire evidence for use in a civil or criminal proceeding? Does it matter if the operator is a private American citizen or a government official? These and related other questions are at the heart of emerging federal and state laws and policies that reflect discomfort with the data gathering and delivery capabilities of UAVs. Several states, in fact, have proposed or enacted laws that preclude drone data from finding their way into civil, criminal, or administrative proceedings. In the modern context of citizen journalists, “selfies,” and police officer body cameras, however, this article argues that singling out drone technology as a matter of law is reactionary and that a robust system of legal rules and practices designed to ensure the reliable, resilient, and uncompromised collection and use of UAV data is imperative.

* Assistant Professor, University of Central Florida, College of Health and Public Affairs, Department of Legal Studies. The author, a Florida Bar Board Certified Aviation Lawyer, presented aspects of this article by invitation at the 2015 Law + Informatics Symposium on Digital Evidence at the Northern Kentucky University Salmon P. Chase College of Law. He is the author of Drone Law (American Bar Ass’n (forthcoming)) and blogs about issues relating to unmanned aerial system at www.droninglawyer.com. Thanks to Stephanie Blum, Jeffrey M. Schmitt, Brian Sites, and Matthew Tokson for their considered comments on earlier drafts of this article. The views expressed herein are solely those of the author, who invites comments at timothy.ravich@ucf.edu or via twitter @ravichaviation.
This article is the first to examine digital information obtained by unmanned, remotely-piloted or optionally manned aviation machines under the rules of evidence and discovery in civil and criminal cases. This analysis combines an introduction and evaluation of drone technology basics with the study of doctrinal legal subject matter such as tort, property, and criminal law, together with notions of personal privacy under state law and the United States Constitution. While the law obviously lags behind technology generally and in the arena of drones specifically, this article contends that current procedural and evidentiary rules are elastic enough to stretch and accommodate the latest advance in information technology.

I. INTRODUCTION

Big changes to traditional legal theories and processes are coming from an unexpected byproduct of the nanotechnology revolution—airplanes, small automated ones. The innovation of unmanned aerial vehicles (“UAVs”) is not flight but information.¹ UAVs—many of which are commercially available, weigh under five pounds, and are widely available—represent data in action. Through algorithms that facilitate the capture and analysis of data, UAVs obtain high-definition enhanced resolution photographs, multispectral and thermal images, volumetric measurements, and top-down real time orthographic and high-accuracy three dimensional topographical maps that can be uploaded onto a thumb drive or into the digital cloud for sophisticated data analytics. Fundamentally, then, UAVs are aerial platforms on which to deploy the latest and most sophisticated hardware and software information-gathering gadgets.

UAVs are as easy to use as handheld computers, iPhones, tablets, and HD cameras on “smart” phones. Some lawmakers, academics, and civil liberties groups are suspicious about whether and how data generated by UAVs could be used in fundamental social processes, however, not least of which are criminal prosecutions and civil lawsuits. This article evaluates how federal and state laws treat UAV-acquired data, leaving to one side complex issues under Fourth

¹. UAVs range from single- and multi-propeller “quad-copters” to engine-driven jets to stealthy, weaponized combat vehicles. They can take-off traditionally via runway or be launched into the air by hand or by catapult device. Landing is accomplished through similar means, including novel and emerging “catch-and-release” systems. Operational versatility aside, lawmakers have struggled to answer the fundamental question of what a drone is, leaving manufacturers, operators, insurers, and even regulators themselves uncertain about the rules that can or should govern the innovation of unmanned aviation. Indeed, federal law and related federal aviation regulations—“FARs”—do not define “drones,” UAVs, unmanned aerial systems (“UASs”), optionally-piloted airplanes (“OPAs”), remotely piloted airplanes (“RPAs”), or remotely controlled airplanes (“RCs”) as a stand-alone category of flying machine. In any case, “unmanned aircraft systems,” or “UASs,” is more accurate terminology for unmanned aerial vehicles, reflecting the fact that the unmanned aerial vehicle is but the airframe component of a coordinated system of associated ground-based personnel and equipment, including flight crew, air traffic control, and so forth. See, e.g., Graham Warwick & Bettina H. Chavanne, Skin in the Game, AVIATION WK. & SPACE TECH., Aug. 10, 2009, at 56.
Amendment jurisprudence in order to focus more specifically on the legislative and regulatory impulse to treat drones differently from similar ground-based data-collecting technologies under procedural and evidentiary rules. Indeed, UAV-obtained digital material is and can be designed to be reliable, resilient, and uncompromised for use in civil and criminal lawsuits, from pre-suit investigation and discovery through trial and appeal. This issue is important given the widespread availability of UAVs, both for private citizens and state and federal law enforcement outfits.

Technically regarded as aircraft,2 civil and commercial UAVs—popularly, though derisively referred to as “drones”—are artificially intelligent devices capable of serving a limitless number of people, industries, and activities. For example, by collecting impactful data, UAVs enable farmers to transform aerially-obtained information into business decisions related to crop health, empower insurers to assess damage in real-time and resolve claims on-site, and allow construction and mining companies to arrive remotely at solutions in managing equipment and operational logistics.3 In other words, UAV owners and operators can get to more places with more agility and at less cost than by using other intelligence, surveillance, and reconnaissance (“ISR”) manned aviation devices. And, the best part—or for aviation regulators and the judiciary, most worrisome part—is that UAVs are accessible to almost anybody at any location at every price point at any time.4 The operational versatility of UAVs, coupled with related tort- and property-based concerns along the lines of privacy and trespass, have prompted several state lawmakers to ban or restrict drone data in

2. Whether a drone was an “airplane” as a matter of law, subject to regulatory enforcement by the Federal Aviation Administration, or a “model airplane” subject to mere policies issued by aviation regulators was largely unresolved until the decision of Huerta v. Pirker. See Huerta v. Pirker, CP-217, Board’s Decisional Order No. EA-5730 (Nat’l Transp. Safety Bd. Decisions (N.T.S.B.) Nov. 18, 2014), available at http://www.ntsb.gov/legal/alj/OnODocuments/Aviation/5730.pdf. According to the National Transportation Safety Board, “[w]hen Congress enacted the Federal Aviation Act of 1958 (which created the Federal Aviation Agency) and defined ‘aircraft’ in the predecessor provision of 49 U.S.C. § 40102(a)(6), so-called ‘drones’ were largely the currency of science fiction. Congress demonstrated prescience, however, in the early definition of ‘aircraft’; it expressly defined the term as any airborne contrivance ‘now known or hereafter invented, used, or designed for navigation of or flight in the air.’ . . . [t]he definition’s use of the passive voice in describing a device that is ‘used’ for flight does not exclude unmanned aircraft. If the operator of an unmanned aircraft is not ‘using’ the aircraft for flight and some derivative purpose—be it aerial photography or purely recreational pleasure—there would be little point in buying such a device. In summary, the plain language of the statutory and regulatory definitions is clear: an ‘aircraft’ is any device used for flight in the air.” See generally Fed. Aviation Admin., MODEL AIRCRAFT OPERATIONS available at https://www.faa.gov/uas/model_aircraft/ (“Model aircraft operations are for hobby or recreational purposes only.”).

3. See, e.g., Philip McNamara, Are Drones a Fad or Here for Good?, TECHCRUNCH (Mar. 5, 2015), http://techcrunch.com/2015/03/05/drones-a-fad-or-here-for-good/.

4. See generally id. (noting that “drone” is a household word and that over 200,000 drones were sold monthly in 2014).
court proceedings.\(^5\) In addition to a federal ban on commercial drone activity,\(^6\) such sweeping anti-drone laws enacted at the state level to date are more populist than potent.\(^7\)

Among these laws are rules disallowing criminal law judges from admitting into evidence any information obtained by drone.\(^8\) Additionally, a private right of action is available to certain litigants to prevent civil or criminal prosecutions based on or informed by drone activity.\(^9\) Both the language and policy advanced by such laws are curious in an era of automated license plate readers,\(^10\) crime scene laser mapping,\(^11\) police officers outfitted with body cameras,\(^12\) and


6. Essentially, the Federal Aviation Administration (“FAA”) disallows private, “civil,” and commercial drone operations. There are presently three methods of gaining FAA approval for flying civil (non-governmental) UAV: First, civil drone operators may apply for a Special Airworthiness Certificates – Experimental Category (SAC-EC) for civil aircraft to perform research and development, crew training, and market surveys. However, carrying persons or property for compensation or hire is prohibited. Alternatively, civil UAS operators may petition the FAA to obtain a UAS type and airworthiness certificate in the Restricted Category (14 CFR § 21.25(a)(2) and § 21.185) for a special purpose or a type certificate for production of the UAS under 14 CFR § 21.25(a)(1) or § 21.17. Or, last, UAS operators may petition for Exemption with a civil Certificate of Waiver or Authorization (“COA”) for civil aircraft to perform commercial operations in low-risk, controlled environments. See FED. AVIATION ADMIN., UNMANNED AIRCRAFTS SYSTEMS (UAS) FREQUENTLY ASKED QUESTIONS, available at https://www.faa.gov/uas/faq/#qn4.

7. See note 5.
8. Id.
9. Id.
11. See generally Victor Li, Data-Driven, 100 A.B.A. J. 17 (2014).
12. See David A. Harris, Picture This: Body-Worn Video Devices (Head Cams) as Tools for Ensuring Fourth Amendment Compliance by Police, 43 Tex. Tech. L. Rev. 357 (2010). Reciprocally, citizens with “smart” cameras are themselves equipped to be “citizen journalists” with the power to watch and record and discipline police behavior. See, e.g., Taylor Robertson, Lights, Camera, Arrest: The Stage is Set for a Federal Resolution of a Citizen’s Right to Record the Police in Public, 23 B.U. PUB. INT. L.J. 121, 148 (2014) (“A federally mandated rule that clarifies the contours and limitations of the right to record will not only spare the courts from contentious litigation about qualified immunity or open-surreptitious inquiries, but it will also educate all of the necessary actors in hopes of ensuring the law’s proper application.”).
communities of drivers prosecuted and fined on the basis of presumptively incontrovertible evidence produced by static red-light cameras.\textsuperscript{13} The disparate treatment of drone technology by some states from other automated surveillance devices appears reactionary and incompletely thought out. \textsuperscript{14} Why indeed should an unprofessional “selfie” taken by a citizen journalist be admitted into evidence in a lawsuit while drone-obtained information—sufficient for purposes as important as national security—are per se banned or severely limited? Additionally, on what principled basis can or should the law discriminate for or against modes of information collection?

To be sure, the ability of drones to surveil people and places for extended periods of time and in invasive ways explains restrictive drone laws. There is an open question, too, whether society should permit law enforcement to use drones up to the Fourth Amendment’s limits, or whether society should bar the police use of drones, or something in between. And, whether private drone footage can be used in criminal, civil, and administrative processes in all circumstances or in none is unclear. This article acknowledges these questions and recognizes that its thesis—that state laws against drone evidence deprives society of relevant, probative, and reliable evidence—cannot be divorced from an analysis of the privacy concerns that have motivated some states to pass restrictive drone laws. Recognizing without trying to resolve these important issues, this article broadly aims to contribute a descriptive overview of drone law in the context of informatics and to suggest that drones can be integrated and accepted into social and legal processes to the same degree as other initially objectionable technologies.\textsuperscript{15}

Moreover, in the absence of any scholarship examining the impact of drones on legal proceedings, this article forwards the position that the adverse reaction by many state lawmakers on both sides of the ideological and political spectrum to UAV technology, perhaps stemming from a fear of the unknown, misunderstands the resilience of existing rules of evidence and procedure. Rule makers, perhaps more than the rules themselves, need rebooting. The legal regime designed around UAV operations can prove critical in the quality of civil and criminal dispute resolution around the nation. In addition to existing protocols, the nation’s laws need to and can be drafted without extensive reworking to embrace, utilize, and harness UAV technology in a socially optimal

\textsuperscript{13} See, e.g., Nicole Kuncl, Seeing Red: The Legal Backlash Against Red-Light Cameras in Florida, 64 FLA. L. REV. 1783, 1788 (2012). See also Robertson, supra note 12, at 148.

\textsuperscript{14} E.g., Ravich, supra note 5.

\textsuperscript{15} Blood, urine, and breath tests, after initially being rejected, have gained judicial support, as have radar equipment, ballistic examinations, and handwriting, fingerprint, footprint, and hair sample analyses. See, e.g., John F. Decker & Joel Handler, Voiceprint Identification Evidence—Out of the Frye Pan and Into Admissibility, 26 AM. U. L. REV. 314, 314 (1977). That these tools and investigative techniques have over time become regular evidentiary features in civil and criminal judicial proceedings is a hopeful precedent, perhaps, for drone technology. On the other hand, lie detector tests have been rejected by the courts for over 50 years. See id. at 315.
way. If clear, workable, and routinized ways of incorporating the byproducts of UAV operations into legal processes are put in place, UAV functionality may enhance and not hinder the adjudicative process.  

This argument is developed in four parts. Given that this article is written in the context of an informatics symposium on digital evidence and the law, Part II generally relates how aviation law interfaces with the discipline of informatics. Part III more specifically evaluates traditional uses of digital evidence in aviation cases as a predicate for Part IV, which analyzes the salient issues that influence the question of the use of information obtained by drones in civil, criminal, and administrative processes. Finally, Part V concludes that a better legal and policy approach than restricting drone evidence unduly is possible and can be achieved by applying the same evidentiary standards to drone forensics as now apply to data and information gained or produced by aerial surveillance generally and other technologies such as cameras, smart phones, and computer-generated visual evidence.

II. THE INTERSECTION OF INFORMATICS AND AVIATION

Defined as “the study of the structure and properties of information, as well as the application of technology to the organization, storage, retrieval, and dissemination of information,” informatics is about putting “technology to work to solve complex problems.” From Facebook to automobile navigation systems to clinical trials to political polling to financial market analysis, “[t]he applications made possible by coupling information with computing technology seem endless.” Unmanned aviation falls squarely within these definitions of informatics. UAVs bring substantial value to a broad span of private and public missions by serving and connecting varied subject matters and economic spaces through aerially deployed sensor suites and software solutions. Thus, informatics—or perhaps legal informatics—may be the discipline best suited to

16. See generally David W. Opderbeck, Drone Courts, 44 Rutgers L.J. 413 (2014) (arguing for a “drone court” of very limited jurisdiction that would nevertheless provide more public accountability than the Foreign Intelligence Surveillance Court).


19. See Informatics: An Interdisciplinary Major at the University of Michigan, Univ. Mich., http://informatics.umich.edu/ (last visited Apr. 3, 2015) (explaining the interdisciplinary major of informatics) (“Think Facebook, automobile navigation systems, clinical trials, online marketing, internet searches, medical imaging, risk assessment, disaster preparedness and response, financial market analysis, DNA analysis, artificial intelligence, internet security, online community organizing, smartphone applications, digital archives, medical records storage and retrieval, political polling, supply chain management, real-time weather maps, etc.”).

20. Vern R. Walker et al., Law Schools as Knowledge Centers in the Digital Age, 88 Chi.-Kent L. Rev. 879, 903 (2013) (thinking about the definition of “legal informatics as ‘the application of informatics within the context of the legal environment and as such involve[ing] law-
house the dedicated study and determination of how drone forensics or actionable information generated by UAV technology influences and can be designed to advance social processes such as criminal and civil litigation.

Historically, the study of human limitations and error in airplane operations fell under the rubric of aviation science. “Human factors” is aviation informatics in this sense. It is the aeronautical jargon and term most commonly used to explain the study of human-machine interfacing in general, commercial, and military flight. Aviation and aerospace medicine is a ready example and is particularly important in the era of commercial jets that are unbounded by time zones, rockets that defy gravity and breach the atmosphere, and warplanes that stealthily exceed supersonic speeds.

Today’s aviation machines perform maneuvers at rates that outpace human decision-making and physical tolerances. Since as early as the 1900s, airplane technology exceeded the human physiological envelope as airmail pilots who flew “flying coffins” had a life expectancy of four years, and one in every six pilots was killed. The law regarded aviation as an ultra-hazardous activity to which the doctrine of res ipsa loquitur applied. While nobody seriously challenged the underlying Bernoullian and Newtonian principles underlying powered flight, the early interface between human beings and flying machines was obviously dangerous. Interestingly, automation and artificial intelligence have both improved and complicated manned flight.

Recent tragedies involving advanced commercial airplanes illustrate the fatal consequences that result when airmen are not able to keep up with advanced avionics and tools. In July 2013, for example, Asiana Airlines Flight 214 crash landed in San Francisco following a failed visual approach (e.g., the pilots reportedly were confused in working with autopilot systems). In March 2014, Malaysia Flight 370 mysteriously disappeared after somebody turned off the related organizations (e.g., law offices, courts, and law schools) and users of information and information technologies within these organizations.”) (alteration in original).

21 “Design informatics,” meanwhile, refers to the study of efficient design of aircraft components. Kazuhsia Chiba, Design-Informatics Approach for Intimate Configuration of Silent Supersonic Technology Demonstrator, J. OF AIRCRAFT, Sept. 2012, at 1200-11. For example, design informatics has been proposed for efficient design, in which a design database is constructed for optimization and design information is extracted from the database by data mining. Design information systematizes the design space and facilitates the efficient selection of a compromise solution. Id.


23 See, e.g., Cox v. Nw. Airlines, Inc., 379 F.2d 893 (7th Cir. 1967).

24. Asiana Crash, Rescue Show Need for Training, SFGATE (Dec. 12, 2013, 8:00 PM), http://www.sfgate.com/opinion/editorials/article/Asiana-crash-rescue-show-need-for-training-5060399.php (“The takeaway impression from hearings before the National Transportation Safety Board expands on earlier reports. The jittery pilot wasn’t up to the task. Customary guidance systems, which were turned off for runway construction, left the crew to rely on cockpit automation, which led to more confusion and error. Seat-of-the-pants flying had no role.”).
airplane’s transponder. In February 2015, TransAsia Airways grounded most of its fleet after flight data indicated that pilots manually cut off fuel to the left engine in error after the right engine of a twin turboprop malfunctioned after takeoff. And, shockingly, these tragedies seemingly pale in comparison to events of March 2015, when Andreas Lubitz, a Germanwings copilot, locked himself in the flight deck, set the automated altimeter for the ground, and crashed an airliner into a French mountainside, killing all 150 people onboard. That these particular catastrophes involved Asian airlines and operators is random. These events highlight a universal concern relating to instrumentation or over-instrumentation of global airspace operations. Indeed, the Asiana, Malaysia, TransAsia, and Germanwings disasters touch on a larger point—the apparent failings or causes of these disasters were manual, not mechanical. Ironically, as aviation regulators continuously evaluate the human element in aviation, including how machines can facilitate and augment manned flight, UAV innovators tout automation—the absence of a manned asset—as the chief asset of their product.

Unlike early aviators of the last century who navigated and controlled airplanes manually, modern air traffic controllers and airmen increasingly mediate or manage highly capable automated systems reactively. Similarly, airport security personnel broker technology as agents who go into motion if, or only when, profiling devices, screening systems, wands, and body imaging systems prompt them to conduct further investigation. From an informatics or aviation science perspective, the streamlined and reduced role for aviation industry stakeholders has promoted knowledge management and improved safety and security over time, but the substitution of computers and autopilot systems for manned assets has come at a cost to foundational human factors, including the decline and deterioration of pilot stick-and-rudder skills, situational awareness (e.g., including avoidance of adverse weather and adverse flight conditions such as stalls), and improvisational instincts. Interestingly, the chief economic

29. See Bart Jansen, Pilots’ Focus in the Cockpit Under Scrutiny, USA TODAY, Aug. 22, 2013, at 1A (“Automated flight controls in airline cockpits have become so reliable that safety experts say pilots could become inattentive to rare malfunctions that can lead to crashes.”).
30. See Jenny W. Hsu et al., TransAsia Planes Grounded as Pilots Retrain, WALL ST. J., Feb. 9, 2015, at A14 (“Over the years, there have been cases in which military and commercial pilots
The attractiveness of UAV technology lies in the ability to replace natural elements for electronic know-how. UAVs are designed to lead, not co-manage or co-pilot, missions, presenting all of the advantages of aviation while obviating the costs of formal aviation training and flight school. UAV innovators are thus comfortable with a dominant role for artificial intelligence and automation to an extent that other institutions—the law, specifically—are not.

III. FROM THE “BLACK BOX” TO THE JURY BOX

Increasingly, machines are thinking for themselves, raising important questions about the future role of manual professional activities. The consulting firm McKinsey & Co., for example, reported that self-driving vehicles could eliminate 90% of all auto accidents in the United States, saving thousands of lives and preventing nearly $190 billion in damages and health costs annually. This prediction worries even some lawyers, and not simply a class of personal injury practitioners. A society in which people commute with fully autonomous cars or robot airplanes to jobs that emphasize science, technology, engineering, and math (“STEM”) fuels a concern about the role of lawyers and judges in a technologically-dependent society. Is there a role for legal practitioners to make contributions to the Internet of Things?

Nobody practically contends that lawyering or judging will be automated one day, but “smart” technologies, embodied by UAVs, challenge legal conceptions of fact-finding and represent situations in which the machines cause injury, but when there is no “principal” directing the actions of the machine.”).


33. See, e.g., Daniel E. Harmon, The IOT and Law Practice: How Will the Internet of Things Impact You This Year?, LAW. PC, Jan. 15, 2015 (“The Internet of Things already is proving beneficial in lawyers’ daily activities. . . . [For example:] A client, needing to reschedule an appointment to an early morning time, late the night before notifies the sleeping lawyer’s calendar app via e-mail. The calendar relays the information to the lawyer’s computerized alarm clock. The alarm clock checks the weather and traffic conditions, calculates how long it will take the lawyer to get to the office, and resets the wake-up time accordingly. It also resets the coffee makers at home and at the office, as well as the office thermostat, so that everyone will be comfy at the meeting.”).

34. See, e.g., Lee Anne Fennell, Between Monster and Machine: Rethinking the Judicial Function, 51 S.C. L. REV. 183, 201 (1999) (“One could argue that it is better to have depersonalized justice than personalized injustice. Alternatively, one might argue that if the only objection to a “justice machine” is the fact that its results are computer-generated, the problem could be solved by simply concealing the truth about the judicial process.”).
both an opportunity and a challenge to sharpen the quality of legal decision making via machines.

Make no mistake, a new and irreversible era of the Information Age has arrived for legal practitioners.\(^\text{35}\) For proof, look no further than the local courthouse where numerous activities occur without lawyer and judges interacting in person. Civil and criminal courtrooms are becoming reliant on electronic practices for administrative, procedural, and substantive matters. State and federal litigants initiate lawsuits, file pleadings and motions, and effect service through case management and electronic case filing systems ("CM/ECF").\(^\text{36}\) Meanwhile, judges are mobile, issuing orders not only from the bench, but also electronically based on their review of legal briefs uploaded to cloud-based personal digital assistants.\(^\text{37}\) Lawyers, for their part, work remotely, "telecommute," conduct client interviews, depositions, and hearings via video conferencing applications, and captivate jurors with computer-generated visual evidence. While the expense of courtroom technology makes it unsuitable for all cases, say landlord tenant matters or garden variety contract and tort suits, few subject areas of law benefit more from the application of courtroom informatics, as it were, than aviation litigation cases.

Airplane accident cases regularly include computer-generated visual evidence and interactive video drawn from event data recorders, more commonly referred to as flight data recorders, cockpit voice recorders, and "black boxes."\(^\text{38}\) The presentation of simulations and accident reconstruction is indispensably powerful for aviation plaintiff and defense counsel explaining aerodynamics, air traffic control, meteorological conditions, and other aspects of aerospace science. Indeed, “[c]omputer technology provides litigators the means to depict not only

\(^{35}\) See, e.g., William T. Braithwaite, *How is Technology Affecting the Practice and Profession of Law?*, 22 Tex. Tech. L. Rev. 1113, 1157 (1991) ("Despite the inherently conservative nature of the institution in which they work, lawyers seem to have been surprisingly vulnerable to the charms of office technology.").

\(^{36}\) See *Case Management/Electronic Case Files, PACER, https://www.pacer.gov/cmecf/* (last visited Mar. 22, 2015) ("The Case Management/Electronic Case Files (CM/ECF) system is the Federal Judiciary’s comprehensive case management system for all bankruptcy, district, and appellate courts. CM/ECF allows courts to accept filings and provides access to filed documents online. CM/ECF gives access to case files by multiple parties, and offers expanded search and reporting capabilities. The system also offers the ability to immediately update dockets and download documents and print them directly from the court system.").

\(^{37}\) Ellie Neiberger, *Judge-Friendly Briefs in the Electronic Age*, 89 Fla. Bar J. 46, 46 (2015) ("Screen-reading on the appellate bench will only move closer to the norm when electronic records on appeal become mandatory next year.").

\(^{38}\) See, e.g., Mark Joye, *Big Brother or Big Savior? Here Comes the Black Box*, S.C. Law. Mag., Sept. 2004 (discussing use of "event data recorders" in the automobile industry). Courts routinely admit into evidence or reject information taken from computerized data recorders used in various modes of transportation, including maritime, rail, and automobile. See *Optical Commc’ns Grp., Inc. v. M/V Ambassador*, 558 Fed. Appx. 94 (2d Cir. 2014) (reviewing summary judgment based on a vessel’s Simplified Vessel Data Radar—the maritime equivalent of an airplane’s black box); *Waisonovitz v. Metro-N. Commuter R.R.*, 350 Fed. Appx. 497 (2d Cir. 2009) (evaluating arguments based on data collected from a train’s “event recorder”).
why an accident happened, but also alternate scenarios of how the accident could have been avoided, in an attempt to show who or what was responsible.”

Litigation arising from the crash of Delta Flight 191 was one of the most important cases to incorporate courtroom technology in complex aviation disputes and is an apt case study of the usefulness of computer technology in legal processes vis-à-vis drones.

On August 2, 1985, a Delta Airlines L-1011 crashed on approach to Dallas-Fort Worth International Airport. The airline, together with its insurers and two of the three cockpit crew members’ estates sued the federal government for the loss of the jetliner, contribution and indemnity, and wrongful death. The central contention in the consolidated lawsuits was that the Federal Aviation Administration and the National Weather Service failed to provide the airline’s crew with reports of severe weather and to warn them to fly around the airport or change runways. The resulting trial—considered the longest in aviation history—generated more than 18,000 pages of transcribed testimony, included 49 expert witnesses, and featured the use of computer-generated simulations to support their cases. The government’s defense emphasized that the Delta crew failed to use their own onboard radar to detect the storm and avoid it.

To support its theory, the government produced computer-generated graphics pertaining to the relevant weather conditions, showing a “recreation of the location and development of weather cells near the airport and cells that would have been depicted on the airborne weather radar of the L-1011 aircraft, had the radar been utilized at any of three different tilt settings,” lead counsel for the Department of Justice attorney involved in the litigation recounted. While computer animation had become somewhat common in litigation up to that time, “the Justice Department’s presentation at the Delta Flight 191 trial marked a new milestone in terms of length, sophistication and technology used.”

The U.S. used a disc player and a laptop computer equipped with custom-designed software in its presentation. By using the laptop computer, a witness could display on television monitors facing the

40. See In re Air Crash at Dallas/Fort Worth Airport on August 2, 1985, 720 F. Supp. 1258, 1290-91 (N.D. Tex. 1989) (“Defendant, the United States of America, is entitled to a judgment in its favor inasmuch as Plaintiffs have failed to prove that the United States of America, through its agents, servants or employees, was guilty of any negligence that proximately caused the air crash of DL 191 on August 2, 1985.”).
41. Id.
43. In re Air Crash at Dallas/Fort Worth Airport, 720 F. Supp. at 1290.
44. See Fadely, Computer-Generated Visual Evidence in Aviation Litigation, supra note 39, at 843 n.12.
45. Marcotte, Animated Evidence, supra note 42, at 53.
judge and lawyers any image on the disc almost instantly—also freeze-
action animation without distortion.\textsuperscript{46}

It took nearly two years for the government to prepare its 55-minute
presentation. Crucial to the simulations was a new generation of digital
flight-data recorder on board Delta 191—the first commercial flight to
-crash in a microburst with such a recorder.

The Justice Department used 40 different parameters, such as
acceleration, roll, pitch and heading, to recreate the plane’s flight. The
plane’s cockpit-voice recorder, ground radar images, weather photos
and other pilots’ statements helped complete the government’s picture
of what happened.

. . . .

Three witnesses for the Justice Department were on the stand for
several days using the simulations, charts and photos to illustrate points
to the judge … the flight synchronized to the cockpit-voice recorder
most effectively illustrated the government’s contentions. Not only
could the judge see the plane’s movement in relation to the storm, he
could see the data displayed on Delta 191’s instruments at the time. The
various animations created an eerie feeling of being there, of seeing and
hearing what the crew experienced.\textsuperscript{47}

Significantly, the animation used in the Delta Flight 191 litigation was
admitted not as demonstrative evidence, but as substantive evidence, meaning it
had independent probative value.\textsuperscript{48} Given the stakes, the parties attacked each
other’s computer animations as inaccurate, inappropriate, prejudicial, and thus
inadmissible.\textsuperscript{49} As such, the computerized evidence offered by the parties was
subjected to a battery of evidentiary tests, including the then-applicable \textit{Frye} general-acceptance standard,\textsuperscript{50} and the requirements of Federal Rules of
Evidence 401,\textsuperscript{51} 402,\textsuperscript{52} 403,\textsuperscript{53} 702,\textsuperscript{54} and 901\textsuperscript{55} dealing with issues of authenticity,

\textsuperscript{46} \textit{Id.} at 54 (“Just as consumers mix and match components to create their own stereo
systems, the U.S. lawyers were among the first to adapt laserdisc technology for courtroom use.
The process is called interactive video and has been widely used in industrial and military
training.”).

\textsuperscript{47} \textit{Id.}

\textsuperscript{48} \textit{Id.} at 55.

\textsuperscript{49} \textit{Id.}; see also Elaine N. Chaney, \textit{Computer Simulations: How They Can Be Used at Trial

\textsuperscript{50} \textit{See} Daubert v. Merrell Dow Pharm., Inc., 509 U.S. 579 (1993) (holding that the “general
acceptance” standard expressed in \textit{Frye v. United States} to determine the admissibility of scientific
evidence had been displaced by the Rules of Evidence).

\textsuperscript{51} Federal Rule of Evidence 401 sets out the test for relevant evidence, providing that
“\ldots [e]vidence is relevant if: (a) it has any tendency to make a fact more or less probable than it would
be without the evidence; and (b) the fact is of consequence in determining the action.” Fed. R.
Evid. 401.

\textsuperscript{52} Federal Rule of Evidence 402 establishes the general admissibility of relevant evidence:
“Relevant evidence is admissible unless any of the following provides otherwise: the United States
relevancy, expert testimony, and possible prejudicial or cumulative aspects of the evidence. In this sense, the Delta Flight 191 litigation is an important precedent to consider when thinking about how data and information procured by UAV might be introduced into court proceedings. Indeed, these same rules could be applied to the data and forensics produced by UAVs.

IV. ANALYSIS

In connection with legislation to allow cameras into federal courtrooms, Supreme Court Justice David Souter once remarked, “[t]he day you see a camera come into our courtroom it’s going to roll over my dead body.” Actually, it might hover and fly.

Given their ability to persistently surveil people at an intimate level, drones are primarily controversial from the point of view of privacy and civil rights. Using UAVs to gather information is controversial in a way that is reminiscent of a decades-long national debate about cameras in courtrooms. True, UAVs implicate the added dimension of aviation safety, but drones are essentially cameras and sensors with wings. While both drones and courtroom cameras and police surveillance systems hit a collective nerve connected to the issues of personal privacy and appropriate law enforcement, the public’s general comfort with the prevalence of cameras in public places would seem to extend to drones:

Society appears to be comfortable with cameras in public areas. After the Boston Marathon bombing in April 2013, law enforcement obtained photographs from store surveillance cameras in order to identify the Boston bomber. Rather than public outrage at the excessive use of surveillance cameras for law enforcement purposes, the public demanded that more be done by law enforcement. There was strong public interest in catching the bombing suspects.

---

53. Under Federal Rule of Evidence 403, federal trial judges “may exclude relevant evidence if its probative value is substantially outweighed by a danger of one or more of the following: unfair prejudice, confusing the issues, misleading the jury, undue delay, wasting time, or needlessly presenting cumulative evidence.” FED. R. EVID. 403.

54. The federal rules contemplate the use of expert testimony as follows: “A witness who is qualified as an expert by knowledge, skill, experience, training, or education may testify in the form of an opinion or otherwise if: (a) the expert’s scientific, technical, or other specialized knowledge will help the trier of fact to understand the evidence or to determine a fact in issue; (b) the testimony is based on sufficient facts or data; (c) the testimony is the product of reliable principles and methods; and (d) the expert has reliably applied the principles and methods to the facts of the case.” FED. R. EVID. 702.

55. Federal Rule of Evidence 901 provides that “[t]o satisfy the requirement of authenticating or identifying an item of evidence, the proponent must produce evidence sufficient to support a finding that the item is what the proponent claims it is.” FED. R. EVID. 901(a).

In cities such as Washington D.C. and New York City, cameras are everywhere. Google Earth and satellite technology have become commonplace. Drones equipped with cameras are simply the latest in surveillance technology. The public is not as concerned about government surveillance in public areas as it once was.

Whether our right to privacy is being violated by the increased use of drones by law enforcement is not the true issue. Commercially, the use of drones in the private sector is becoming even more pervasive. The concern is law enforcement abuse—that the government will collect the video and photographs from drone surveillance for a purportedly legitimate purpose only to use this material for other nefarious or illegitimate purposes.57

Indeed, mission creep and the militarized narrative of drones as hunter-killer robots—and the not insignificant fact that drones can be weaponized—reinforces the natural difficulty for some lawmakers and citizens to accept unmanned and optionally-piloted aviation technology in the same fashion other audio and visual evidence-generating machines are regarded. The demonization of drones is amplified, moreover, by regular stories of unscrupulous operators of drones who cause near-collisions with commercial aircraft, engage in sophomoric pranks of flying over sunbathers, or make unpermitted passes over government buildings and historic landmarks such as the Eiffel Tower.59

Stories of irresponsible, criminal, or armed deployments of UAVs attract more attention and interest than the “good” uses of UAVs, including, potentially,

57. Melanie Reid, Grounding Drones: Big Brother’s Tool Box Needs Regulation Not Elimination, 20 RICH. J.L. & TECH. 9, 91-92 (2014). The claim that society is comfortable with pervasive public camera surveillance should be made cautiously without poll data to back it up. Moreover, the fact that some members of society may be willing to exchange privacy for safety after a major terrorist attack likely is not the best indicator of their privacy views in general. All that said, CCTV has been widely accepted in England, and major cities use CCTV in certain areas. Thus, it is possible that Americans could go the English route, but that debate is yet to happen in the United States. See, e.g., Nick Taylor, Closed Circuit Television: The British Experience, 1999 Stan. Tech. L. Rev. 11 (1999).


60. See, e.g., Kurtis Lee, Drones to be Disabled in Central D.C., L.A. TIMES, Jan. 29, 2015, at A11 (reporting that the manufacturer of a drone that crashed on the White House grounds in January 2015 plans to install software in its devices that would prevent them from flying in much of Washington).

evidence generation for criminal and civil law purposes. The advantageous application of drones are hard to imagine in legal processes because the innovation is bedeviled by important Constitutional, privacy, law-enforcement, and safety concerns.

But, drones could optimize substantive judicial processes by enhancing the quality of evidence that could be presented to a judge or jurors. Consider the ability of UAVs to take pictures and record video imagery in public places. Drones that record property damage, for example, would offer probative evidence for fact-finders in any tribunal. Thus, rather than banning UAVs outright (as Virginia initially did) or conditioning any or all drone use on the issuance of a probable cause warrant and/or occurrence of extraordinary and all but unpredictable events involving national security or terrorism, incorporating provably reliable drone technology into existing procedural and evidentiary rules would promote the fact-finder’s objective. Indeed, from a policy perspective, asking how the use of drone-gathered data could be helpful for the adjudication of civil, criminal, and administrative matters is a more productive exercise for lawmakers than preoccupying with hypothetical Palsgrafian scenarios involving rogue robot airplanes.

A. Common and Constitutional Law Considerations

The argument that drones can and should be incorporated into legal processes should not be understood to mean that doing so is or will be easy. On the one hand, traditional tort concepts such as trespass can encompass UAV operations. With respect to trespass and property rights, for example, discussions about integrating UAVs into the national airspace system (“NAS”) echo legal controversies from two centuries ago respecting ground rights with air rights. In Guille v. Swan, a property owner sued after the operator of an air balloon crashed-landed into his garden in New York City. “When the balloon descended [the balloonist called for assistance and] more than two hundred persons broke into [the] garden through the fences, and came onto the premises [to his rescue], beating down [the garden’s] vegetables and flowers.” Applying traditional conceptions of property and trespass to the advent of aviation, the Guille court reasoned that the balloonist was strictly liable for trespass. That is,

ascending in a balloon is not an unlawful act . . .; but, it is certain, that the aeronaut has no control over its motion horizontally; he is at the sport of the winds and is to descend when and how he can; his reaching the earth is a matter of hazard. He did descend on the premises of the plaintiff below, at a short distance from the place where he ascended.

---

62. Reid, supra note 57, at 94.
64. Id. at 381.
Now, if his descent, under such circumstances, would, ordinarily and naturally, draw a crowd of people about him, either from curiosity, or for the purpose of rescuing him from a perilous situation; all this he ought to have foreseen, and must be responsible for.65

Guille simply reflected an early view of aviation—whether by balloon or something else—as ultra hazardous activity.66 The law has evolved since Guille in the form of aviation-specific regulations that prohibit any person from operating an aircraft below 1,000 feet above any congested area or below 500 feet above the surface.67 What remains unresolved—and more difficult to resolve—are privacy and Fourth Amendment issues arising under the Constitution vis-à-vis drone operations.

The seminal case Florida v. Riley68 illustrates the difference in regulatory treatment between accepted aviation technologies and UAVs. The issue in Riley was whether a search under the Fourth Amendment had occurred when a police helicopter flew 400 feet above a residential greenhouse to observe contraband.69 The Supreme Court of Florida held that helicopter surveillance at 400 feet constituted a search for which a warrant was required, but the Supreme Court of the United States disagreed. Justice Byron White wrote that "[t]he Fourth

65. Id. at 383. More than a century later, the rule expressed in Guille, that the doctrine of strict liability controls legal disputes concerning injuries caused by aircraft to persons and things on land, was reformulated:

- If physical harm to land or to persons or chattels on the ground is caused by the ascent, descent or flight of aircraft, or by the dropping or falling of an object from the aircraft,

(a) the operator of the aircraft is subject to liability for the harm, even though he has exercised the utmost care to prevent it; and
(b) the owner of the aircraft is subject to similar liability if he has authorized or permitted the operation.


66. Compare Rochester Gas & Elec. Corp. v. Dunlop, 266 N.Y.S. 469 (N.Y. Co. Ct. 1933) (finding strict liability for trespass and property damaged caused by airplane crash), with Crist v. Civil Air Patrol, 278 N.Y.S.2d 430, 434 (N.Y. App. Div. 1967) (declining application of strict liability or doctrine of res ipsa loquitur in absence of showing of intent to crash airplane and noting that “[t]echnological advances and development, and the experiences of the last two decades have dissipated the universal early fears that flying was an ultra hazardous occupation. The application of the trespass theory advanced in the Dunlop case appears to be based to some extent on a recognition of such earlier fear.”).


69. Id.
Amendment simply does not require the police traveling in the public airways at this altitude to obtain a warrant in order to observe what is visible to the naked eye.”

Riley concerned what could be seen with the naked eye from a helicopter in the national airspace system, however it would seem to allow drone operations for law enforcement purposes insofar as the flying properties of quadcopter drones and helicopters is similar. And, while decisions concerning personal privacy protections share a common ancestor in Katz v. United States, case law respecting aerial observation and surveillance is intensely fact specific and irregular. For example, in California v. Ciraolo, the Supreme Court of the United States concluded that, “[i]n an age where private and commercial flight in the public airways is routine, it is unreasonable … to expect that [ ] marijuana plants were constitutionally protected from being observed with the naked eye from an altitude of 1,000 feet.” In this respect Ciraolo and Riley seem to allow UAV operations for like law enforcement purposes, but, in fact, the law does not yet say what reasonable privacy expectations, if any, attach to unmanned airplane operations. Riley and Ciraolo and references to the “naked eye,” moreover, apply to manned aviation, and almost by definition, do not extend to surveillance technologies that perform out of the visual line of sight of its operators.

Additionally, more recent rulings by the nation’s high court have extended Fourth Amendment protections to sense-enhancing technologies, potentially impacting drone missions significantly. In Kyllo v. United States, for example, the Supreme Court addressed the public use of invasive technologies and found that use of thermal imaging devices to search a residence was improper under the Constitution. Kyllo only applies to devises used to find facts about the interior of a home; presumably, then, drones could be used to find facts about backyards and the like without violating the Kyllo. Alternatively, in United States v. Jones, 75 for example, the Environmental Protection Agency’s use of a commercial aerial photographer, and standard floor-mounted, precision aerial mapping camera, to take photographs of a chemical company’s industrial complex within the navigable airspace, at altitudes of 12,000, 3,000, and 1,200 feet was not a search prohibited by the Fourth Amendment). 76

---

70. Id. at 450.
73. California v. Ciraolo, 476 U.S. 207 (1986). See also Dow Chem. Co. v. United States, 476 U.S. (1985) (finding that the Environmental Protection Agency’s use of a commercial aerial photographer, and standard floor-mounted, precision aerial mapping camera, to take photographs of a chemical company’s industrial complex within the navigable airspace, at altitudes of 12,000, 3,000, and 1,200 feet was not a search prohibited by the Fourth Amendment).
76. United States v. Jones, 132 S. Ct. 945 (2012). See, e.g., Sean M. Kibane, Note, Drones and Jones: Rethinking Curtilage Flyover in Light of the Revived Fourth Amendment Trespass Doctrine, 42 CAP. U. L. REV. 249 (2014) (“In aerial surveillance cases, the ultimate decision as to whether vertical curtilage of the home receives such protection depends on if the Supreme Court declares vertical curtilage of the home to be a constitutionally protected area”); Timothy T.
a physical trespass case, the Supreme Court disallowed searches using the very type of equipment that might be deployed on a drone, including radio transmitters, receivers, high resolution digital video cameras, and navigation and global position tracking devices. And, in *Florida v. Jardines*, the Supreme Court essentially equated a dog with a sensor and found unconstitutional law enforcement’s use of a drug-sniffing canine to investigate an unverified tip that drugs were being grown at a residence. 77 *Jardines* is tied to the Supreme Court’s finding that there was a physical trespass of a residence, a finding that could apply to unauthorized flight of drones over someone’s property. Finally,

The First Amendment of the Constitution also is implicated to the extent that the data collected, stored, analyzed, and reported by drones constitutes speech—"data speech." 78 Also, the idea that a machine’s output could be used as evidence against a civil litigant or criminal defendant may run afoul of the Constitution’s Confrontation Clause:

Under the current interpretation of the Confrontation Clause ... the right to cross-examine some individuals, especially in the forensic setting, faces an approaching extinction. Science increasingly delivers machines possessing fully automated processes such that the only people who contribute to the machine’s speech are the progenitors. This effective expiration date on a portion of the Confrontation Clause is a possibility … but that, in time, will arrive. It is not unusual for constitutional rights to contract and expand in the face of technological change; Fourth Amendment jurisprudence has long recognized that fact. The current status quo is, nonetheless, troubling. For now, that expiration has not arrived because some machines still require analyst input; the dawn of fully autonomous machines has not yet arrived. But the horizon is a familiar orange, and the sun is steadily ascending; the rise of the machines has only begun. 79

---

78. See, e.g., Jane Bambauer, *Is Data Speech?*, 66 STAN. L. REV. 57, 60 (2014) (examining when factual information becomes speech and contending that “freedom of speech carries an implicit right to create knowledge”); Andrew Tutt, *The New Speech*, 41 HASTINGS CONST. L.Q. 235, 236 (2014) (“While the disruptive technologies of the past helped to make information available more widely, more quickly, or more permanently … digital technology also stands to grant unprecedented individuated control to the intermediary who carries that information.”). See also David Goldberg et al., *Remotely Piloted Aircraft Systems & Journalism: Opportunities and Challenges of Drones in News Gathering*, UNIV. OXFORD, REUTERS INST. FOR STUDY JOURNALISM (2013), available at https://reutersinstitute.politics.ox.ac.uk/sites/default/files/Remotely%20Piloted%20Aircraft%20and%20Journalism.pdf (summarizing the “technical, policy, and journalistic issues that need to be comprehended before [drones] are used for news gathering”).
Presuming overarching common law (e.g., trespass, privacy) and Constitutional issues presented by UAV technology do not otherwise or obviously present, existing protocols for the acquisition and presentation of evidence—in public spaces, for example—can and should apply to the data deliverables generated by autonomous aerial vehicles.

B. One Nation, Against Drones

For drones, the sky is not the limit, but state legislatures might be.80 Indeed, from a legal informatics perspective, the digital evidence that UAVs are capable of offering is as promising as the legal regime evolving around small autonomous aerial vehicles is restraining. Notwithstanding their transformative capabilities, drones activate privacy concerns by a public already apprehensive about reports of federal government surveillance programs involving personal cell phone records in contravention of the Fourth Amendment in the name of national security.81 State lawmakers, too, are confronting the national challenge of balancing privacy rights against security needs.82 Overwhelmingly, in an era where cellphones can capture evidence and scenes freely, states have codified

80. See, e.g., Nate Vogel, Drones at Home: The Debate over Unmanned Aircraft in State Legislatures, 8 ALB. GOVT’L L. REV. 204, 231 (2015) (“Legislators in forty-six states and Puerto Rico have introduced almost 200 bills that relate to unmanned aircraft during legislative sessions from 2011 to 2014 … there is little national consensus about how unmanned aircraft should be regulated; there are hundreds of ideas, but no widely recognized solutions.”).

81. See Delvin Barrett, CIA Aided Program to Spy on U.S. Phones, WALL ST. J., Mar. 10, 2015, at A1, available at http://www.wsj.com/articles/cia-gave-justice-department-secret-phone-scanning-technology-1426009924 (explaining that the Department of Justice reportedly runs a program that operates specifically equipped planes that fly from five U.S. cities, with a flying range covering most of the U.S. population) (“The CIA and the U.S. Marshals Service, an agency of the Justice Department, developed technology to locate specific cellphones in the U.S. through an airborne device that mimics a cellphone tower.”). The devices—dubbed “dirt boxes” by law enforcement officials, trick cellphones into reporting their unique registration information. See id.; see also Margo Schlanger, Intelligence Legalism and the National Security Agency’s Civil Liberties Gap, 6 HARV. NAT’L SEC. J. 112, 205 (2015) (“In this post-Snowden moment, Congress can and should protect Americans’ privacy and civil liberties by clamping down on bulk surveillance, creating legal rules that can then be enforced by the courts and the intelligence community’s large compliance bureaucracy. But Congress and the President should not be limited by intelligence legalism. They should also follow the quite different strategy of amplifying voices inside the surveillance state who will give attention in internal deliberations and agency operations to civil liberties and privacy interests. But institutional design is important; civil liberties offices need deliberate and careful arrangements to safeguard their influence and commitment.”) (Alteration in original.)

82. See, e.g., Dawn M. K. Zoldi, Drones at Home: Domestic Drone Legislation—A Survey, Analysis and Framework, 4 U. MIAMI NAT’L SEC. & ARMED CONFLICT L. REV. 48, 81 (2014) (“A review of state drone bills, current DoD domestic IO policies and existing Constitutional principles highlighted that the focus of legislative activity remains on government actors, with an emphasis on law enforcement. There is with little regard for the second and third order effects of others with significant equities in domestic drone use, particularly the U.S. Armed Forces. The way ahead for future law and policy is simple: differentiate between users; focus on the purpose of the collection; and apply already existing relevant principles.”).
laws that disallow the warrantless use of UAVs for purposes of obtaining evidence for use in court.\(^{83}\)

Many states have enacted substantive laws outlawing or restricting UAV operations for all purposes, including law enforcement missions.\(^{84}\) North Carolina and Virginia, for example, initially imposed general moratoria on public UAVs until July 1, 2015.\(^{85}\) Other states have enacted rigid anti-drone legislation, including Florida,\(^{86}\) Idaho,\(^{87}\) Illinois,\(^{88}\) Montana,\(^{89}\) North Carolina,\(^{90}\) Oregon,\(^{91}\) Tennessee,\(^{92}\) Texas,\(^{93}\) and Virginia.\(^{94}\) Most of the laws read almost verbatim.

In Kentucky, for example, state lawmakers proposed House Bill 12, or the “Citizens’ from Unwarranted Surveillance Act” (“CUSA”). The proposed law would define a drone as an “aircraft that is operated without the possibility of direct human intervention from within or on the aircraft.”\(^{95}\) Excepting drones operated by the armed forces of the United States,\(^{96}\) “drones may not be equipped with a lethal payload,” under the proposed statute. Moreover, under the CUSA, law enforcement agencies would be barred from using a drone “to gather evidence or other information, or utilize, disclose, or receive information acquired” by drone absent a search warrant signed a judge.\(^{97}\) In the event of an emergency, “an application for a search warrant approving such operation may be made within forty-eight hours after the operating begins.”\(^{98}\) Additionally, the law would make inadmissible in any civil, criminal, or adjudicative proceeding any “evidence obtained or collected as the result of the use of a drone.”\(^{99}\)

While the proposed CUSA mirrors the enacted laws of other states, it differs in important ways. Florida’s similarly-named statute, for example, affords private litigants the right to sue in civil court “to obtain all appropriate relief in order to

\[\text{83. See id. at 64.}\]
\[\text{84. See id.}\]
\[\text{86. Freedom from Unwarranted Surveillance Act, 2013 Fla. Laws 33.}\]
\[\text{89. MONT. CODE. ANN. § 46-5-109 (2013).}\]
\[\text{96. Id. § 2.}\]
\[\text{97. Id. § 5(a).}\]
\[\text{98. Id. § 5(a).}\]
\[\text{99. Id. § 7.}\]
prevent or remedy a violation."\textsuperscript{100} Kentucky’s law provides no such private remedy, rendering the proposed legislation somewhat toothless and aspirational in a civil context, though perhaps not in a criminal proceeding. That said, the CUSA, or Kentucky House Bill 12, is unique in its prohibition of the use of facial recognition and biometric matching technology collected by a drone.\textsuperscript{101} Additionally, while carving out an exception for higher education institutions to use drones for educational, research, or testing purposes, the proposed law states that “[a]ny business entity doing business lawfully within this state may use a drone for business purposes.”\textsuperscript{102} This provision is a non-starter, however. It runs afoul of the Supremacy Clause of the United States Constitution in that it would be preempted by the Federal Aviation Administration’s ban on commercial UAV operations nationally.\textsuperscript{103}

Enforcing the CUSA may be problematic as a practical matter, too. The proposed law, Kentucky House Bill 12, does not say what burden the government must carry to obtain a search warrant authorizing the use of drones.\textsuperscript{104} While the CUSA may effectively ban warrantless drone surveillance, important questions remain about situations in which the collection of surveillance is arguably a vital exercise of a state’s police power. The CUSA invites authorities to apply for a search warrant within 48 hours of an emergency event that required the use of drones,\textsuperscript{105} but upon what standard? Would “reasonable suspicion” by the government of an emergency situation be sufficient to use a drone for emergency purposes or something more or less stringent? And, if the government were to “cry wolf” and characterize a “regular” crime (or no crime at all) as a terrorist event, what evidence must a judge consider to do anything more than second-guess first responders? In fact, criminal courts will be asked to apply a \textit{per se} exclusion of “evidence and information” obtained by law enforcement drones and make judgment calls like whether a drone was used to counter an actual terrorist attack (an emergency situation potentially within the CUSA) or to deter activities that were terrible but less terrible than a terrorist attack (putatively disallowed the CUSA).\textsuperscript{106}

\textsuperscript{100.} \textsc{Fla. Stat.} \textsection 934.50(5) (2013) (enacted as “[s]earches and seizure using a drone”).
\textsuperscript{101.} H.B. 12 (Ky. 2015) \textsection 6.
\textsuperscript{102.} Id. \textsection 3.
\textsuperscript{103.} See generally, e.g., Jol A. Silversmith, \textit{You Can’t Regulate This: State Regulation of The Private Use of Unmanned Aircraft}, 26 \textsc{Air \\& Space Law.} 1 (2013). \textit{See also} Abdullah v. American Airlines, Inc., 181 F.3d 363, 375 (3d Cir. 1999) (finding that federal law impliedly preempts the entire field of air safety generally, but that state and territorial remedies for violations of federal standard of care apply thereafter). Additionally, and perhaps circular, if a state law prohibits members of the public from flying drones, then their use is not open to members of the public and thus their use may violate a reasonable expectation of privacy. In this regard, state law would change a traditional constitutional privacy analysis. Yet, this also would not seem to be an issue if state anti-drone laws are preempted by federal law.
\textsuperscript{104.} H.B. 12 (Ky. 2015).
\textsuperscript{105.} Id. \textsection 5(a).
\textsuperscript{106.} See id.
In all, the CUSA suffers from the same defect as other state anti-drone laws: they assure a constituency on a red-meat political issue at the expense of legal coherence. Yes, drafting legislation that stimulates new innovations without eviscerating important civil rights is difficult. State drone laws that intend to safeguard personal privacy rights in an era of evermore invasive technologies are desirable in this context. News accounts of “predators” and “reapers” and “hunter killers” deployed to kill ISIS terrorists and enemies in Afghanistan and Iraq are constant. At the same time, President Barack Obama’s comments in a speech delivered at the National Defense University that Americans who go abroad to wage war against America are entitled to no more protection from drones “than a sniper shooting down on an innocent crowd should be protected from a SWAT team” are troubling. Enacted and proposed laws like the CUSA are big on announcing broad restrictions in reaction to such pronouncements but small on providing details essential for enforcement. Undefined are what kinds of “evidence or information” state law enforcement agencies are prohibited from gathering, be it an aerial photograph of something open and obvious like a building or home or something for which no reasonable expectation of privacy exists.

C. No Drone is Above the Law

The first generation of state drone laws collectively misapprehends that when it comes to aviation regulations respecting safety and airspace, federal law

---

108. Remarks by the President at the National Defense University, WHITE HOUSE OFFICE OF THE PRESS SECRETARY (May 23, 2013, 3:00 PM), http://www.whitehouse.gov/the-press-office/2013/05/23/remarks-president-national-defense-university. See generally Milena Sterio, The Covert Use of Drones: How Secrecy Undermines Oversight and Accountability, 8 ABL. GOV’T L. REV. 129, 164 (2015) (arguing that the Central Intelligence Agency “could provide more policy and legal guidelines about its targeting operations as a general matter, without prejudicing the likelihood of success of any specific operation”); Laurie R. Blank, After “Top Gun”: How Drone Strikes Impact the Law of War, 33 U. PA. J. INT’L L. 675, 716-17 (2012) (“Use of armed drones continues to raise serious questions about the numbers and nature of civilian casualties, but these questions stem primarily from the procedures for selecting targets and approving attacks, not from the nature and capabilities of drones themselves. As with any other weapon, it is essential to ensure that UAV attacks are launched only against legitimate military objectives in accordance with the obligations of proportionality and precautions.”); Thomas M. McDonnell, Sow What you Reap? Using Predator and Reaper Drones to Carry Out Assassinations or Targeted Killings of Suspected Terrorists, 44 GEO. WASH. INT’L L. REV. 243, 315-16 (2012) (“Despite the decapitation of numerous Taliban and al Qaeda leaders and the Obama administration’s belief that the strikes have effectively paralyzed al Qaeda in the Pakistan tribal areas, there is some evidence to suggest that such operations might actually strengthen such organizations both internally and externally. Employed against these targets, the unchivalrous, seemingly cowardly, method of warfare might result in greater support for terrorists and more terrorist recruits in the Islamic world.”).
prevails over and preempts state enactments. Whether and where UAVs are permitted to fly in the national airspace system is a matter of federal law, a power of the federal government found in the Supremacy Clause of the Constitution.

Current airspace regulations originate in Roman law, which supported the concept that ownership of land extended to the periphery of the universe as expressed in the ancient doctrine *cujus est solum ejus usque ad coelom*—”whoever owns the soil, it is theirs up to Heaven.” This doctrine was originally a part of the American common law, but abandoned in the case of *United States v. Causby*. The controversy arose when a North Carolina farmer sued the federal government for inverse condemnation under the Fifth Amendment on the basis that the operation of army and navy aircraft at low altitudes above his farm produced light and noise that not only terrified his family but caused his chickens to kill themselves from fright, resulting in the destruction of the use of his property as a commercial chicken farm.

The federal government argued that no taking had occurred under the Constitution under the authority of the Air Commerce Act of 1926. Pursuant to that law, the United States has “complete and exclusive national sovereignty in the air space” over the country while private citizens have “a public right of freedom of transit in air commerce through the navigable air space of the United States.” Given that “navigable air space” includes “airspace above the minimum safe altitudes of flight prescribed by the [FAA],” the government argued in *Causby* that its flights were merely an exercise of the right of travel.

---

109. *See, e.g.*, Troy A. Rule, *Airspace in An Age of Drones*, 95 B.U. L. Rev. 155, 208 (2015) (advocating for the application of “principles of microeconomics and property theory [which] call for new laws giving landowners more definite rights to exclude drones from the airspace directly above their land. These exclusion rights would be most effective if they were treated as equivalent to rights that landowners have long enjoyed in surface land and if they extended all the way up to the navigable airspace line where the public highway for air travel begins”).

110. *See generally* Timothy M. Ravich, *The Integration of Unmanned Aerial Vehicles into the National Airspace*, 85 N.D. L. Rev. 597, 621 (2009) (“Until a single policy is adopted, the emergence of UAVs presents nearly a clean slate for lawmakers to craft a regulatory environment that enhances the interrelated objectives of commerce, safety, and national security.”).

111. *United States v. Causby*, 328 U.S. 256, 260-61 (1946). *See also* Nw. Airlines, Inc. v. Minnesota, 322 U.S. 292, 302-03 (1944) (Jackson, J., concurring) (“Aviation has added a new dimension to travel and to our ideas. The ancient idea that landlordism and sovereignty extend from the center of the world to the periphery of the universe has been modified. Today the landowner no more possesses a vertical control of all the air above him than a shore owner possesses horizontal control of all the sea before him. The air is too precious as an open highway to permit it to be ‘owned’ to the exclusion or embarrassment of air navigation by surface landlords who could put it to little real use.”).

112. *Causby*, 328 U.S. at 259.

113. *Id.* at 260.


116. *Id.*
through the airspace within the minimum safe altitudes for flight. Because the flights occurred within the navigable airspace without physically invading the farmer’s property, the government argued, its military flights did not constitute a taking, but at most caused only incidental damage as a consequence of authorized air navigation. The United States Court of Federal Claims rejected this argument, awarding $2,000 as for the value diminution of the farmer’s land, upon which an avigational easement or servitude had been imposed.

While the Supreme Court of the United States upheld the lower court’s finding that a taking had occurred, it remanded the issue of damages for a specific description of the nature of the taking, including whether it was temporary or permanent. In doing so, the Court’s majority recognized the transformative properties of aviation, both practically and legally: “The airplane is part of the modern environment of life” where ancient doctrines of airspace ownership such as ad coelom “ha[d] no place in the modern world. The air is a public highway … Were that not true, every transcontinental flight would subject the operator to countless trespass suits.” At the same time, the Court recognized the need to balance aviation operations against traditional conceptions of property rights; “if the landowner is to have full enjoyment of the land, he must have exclusive control of the immediate reaches of the enveloping atmosphere.” Otherwise, if private land owners were denied access to the “superadjacent airspace,” then “buildings could not be erected, trees could not be planted, and even fences could not be run.”

The central controversy in Causby thus involved traditional private property rights, on the one hand, against the emergence of national airways or highways in the sky.

To resolve the dispute, the Causby Court noted the fact that no traffic rules placing the airspace needed for take-off and landing within the public domain had existed by 1946. Accordingly, the Court recognized that it was not asked to rule upon any regulation prescribing 83 feet as the minimum safe altitude. Rather, where government “[f]lights over private land … are so low and frequent as to be a direct and immediate interference with the enjoyment and use of the land,” Justice William O. Douglas stated, the question took on a constitutional dynamic. As such, the Causby Court ruled that even though “the inconveniences which [the airplane] causes are normally not compensable under the Fifth

118. Id.
119. Id. at 259.
120. Id. at 268.
121. Id. at 261.
122. Id. at 264.
123. See United States v. Causby, 328 U.S. 256, 264 (1946).
124. See id. at 263.
125. Id.
126. Id. at 266.
Amendment, a taking effected by the path of glide of government airplanes was no different than more conventional forms of entry onto private property: “We have no doubt that if the United States erected an elevated railway over [the farmer’s] land at the precise altitude where its planes now fly, there would be a partial taking, even though none of the supports of the structure rested on the land.” Under Causby, then, the taking of an avigational easement turned on whether an airplane flew directly over private land, the altitude and frequency of the flights, and whether the flights directly and immediately interfered with the enjoyment and use of the land. This legal analysis has since been applied by other courts in disputes involving airspace use and private property rights.

Causby has enjoyed renewed relevance with the emergence of drones. The question of where UAVs fit into the NAS is a modern day take on the same issue raised in the middle of the last century about where airplanes generally fit into the NAS. A solution, albeit one subject to amendment, was presented in February 2015 when the Federal Aviation Administration (“FAA”) announced rules for the integration of UAVs in the NAS. The FAA proposed under Title 14 of the Code of Federal Regulations to amend its regulations to adopt specific rules to allow the operation of small unmanned aircraft systems in the NAS. These changes would address the operation of unmanned aircraft systems, certification of their operators, registration, and display of registration markings. The proposed rule would also find that airworthiness certification is not required for small unmanned aircraft system operations that would be subject to the proposed rule. Lastly, the proposed rule would prohibit model aircraft from endangering the safety of the NAS. The proposed rule, which is open to public comment and will not be finalized until approximately 2017, requires that the person actually

127. Id.
128. Id. at 264-65.
129. See, e.g., Andrews v. United States, 108 Fed. Cl. 150, 155-56 (Fed. Cl. 2012) (applying Causby analysis to dismiss inverse condemnation claim by a Virginia property owner in connection with overflights by U.S. Navy F/A 18 “Super Hornet” fighter jets). See also RESTATEMENT (SECOND) OF TORTS § 159 (1965) (“[S]pace rockets, satellites, missiles, and similar objects aside, [f]light by aircraft in the air space above the land of another is a trespass if, but only if, (a) it enters into the immediate reaches of the air space next to the land, and (b) interferes substantially with the other’s use and enjoyment of his land.”).
130. See, e.g., Griggs v. Cty. of Allegheny, 369 U.S. 84, 87-90 (1962) (taking when “regular and almost continuous daily flights [occurred] directly over and very, very close to [the] plaintiff’s residence,” made conversations and sleep in the residence difficult, rattled windows, caused plaster to fall from walls and ceilings, and negatively impacted residents’ health).
flying a small UAV would be an “operator.” An operator would have to be at least 17 years old, pass an aeronautical knowledge test and obtain an FAA UAV operator certificate. To maintain certification, the operator would have to pass the FAA knowledge tests every 24 months. A small UAV operator would not need any further private pilot certifications (i.e., a private pilot license or medical rating).

The proposed rule also would impose operating limitations designed to minimize risks to other aircraft and people and property on the ground:

- A small UAV operator must always see and avoid manned aircraft. If there is a risk of collision, the UAV operator must be the first to maneuver away.
- The operator must discontinue the flight when continuing would pose a hazard to other aircraft, people or property.
- A small UAV operator must assess weather conditions, airspace restrictions and the location of people to lessen risks if he or she loses control of the UAV.
- A small UAV may not fly over people, except those directly involved with the flight.
- Flights should be limited to 500 feet altitude and no faster than 100 mph.
- Operators must stay out of airport flight paths and restricted airspace areas, and obey any FAA Temporary Flight Restrictions.

With these rules in place, eventually, UAV operations are likely to be as routine and accepted as other aviation operations.

D. UAV Evidence is Evidence

As some lawmakers across the nation hastily move to implement rules prohibiting the admission of drone-acquired information, modifying, amending, and extending existing rules of procedure and evidence to accommodate UAV technology would be more productive. Indeed, existing rules provide a firm framework within which to assess the quality and use of UAV-obtained evidence, including core concepts like relevancy, reliability, hearsay, the best evidence rule, and the rule against introducing unfair prejudice.

134. Id. at 9546.
135. Id.
136. Id.
137. Id. at 9567.
138. Id. at 9546-47.
139. See note 5 and accompanying text, supra.
140. See Fadeley, supra note 39, at 893 (“The printout from a computer is considered an original. This objection also is easily overcome.”).
confusion, or cumulative evidence. These evidentiary tools are in addition to counsel’s opportunity to establish admissibility of computer evidence through stipulation or a pretrial hearing on admissibility.

_A fortiori_, while UAVs are disruptive of the _status quo_, the information they generate does little if anything to disturb traditional general discovery rules in a civil setting. For example, the federal rules of civil procedure and like-worded state procedural rules allow parties to obtain non-privileged information that is relevant or reasonably calculated to lead to the discovery of admissible evidence.¹⁴¹ No reasons have been presented by lawmakers as to why this well-established procedural rule could not serve as an effective safeguard against untrustworthy UAV data just as it presently serves to vet computer-generated or produced information disclosed during civil litigation. With respect to admissibility of UAV-generated documentary materials, meanwhile, traditional evidentiary principles can and should apply. UAV-generated evidence, be it in statistical, graphical, audio, or visual form, “accomplishes nothing in substance that attorneys have not done in the past through documentary, real, demonstrative, or testimonial evidence.”¹⁴² And, again, Rule 403 of the evidence code would continue to serve as an effective balance against evidence whose probative relevance is outweighed by the risk of unfair prejudice.¹⁴³ Additionally, and practically, the use of drone technology would not favor either side in criminal or civil trials given the availability and affordability of most UAVs.

The introduction of UAV-acquired data also finds precedence in the ways in which lawyers and judges traditionally lay the predicate and establish the foundation of computer-generated materials created specifically for use in litigation, such as breathalyzer results in DUI cases:

>[P]roviding the opponent an opportunity to examine the program, including the proposed input data; showing the equipment is reliable (especially through brand names); and showing the software used is either widely accepted (a standard program) or demonstrating the program produced reliable results. This latter showing may consist of testimony from the individual(s) who prepared the program, their qualifications, an explanation of what the program is designed to perform, including any changes made in the program, and measures taken in order to ensure accurate output. The foundation for a computer model designed for litigation should include more than just an explanation of variables used. Besides identifying the variables, the relationship between the variables should be described, including the

¹⁴². Fadely, _supra_ note 39, at 893.
¹⁴³. _Fed. R. Evid._ 403. Rule 403 provides that, “[a]lthough relevant, evidence may be excluded if its probative value is substantially outweighed by the danger of unfair prejudice, confusion of the issues, or misleading the jury, or by considerations of undue delay, waste of time, or needless presentation of cumulative evidence.” _Id._
weight given to any specific variable since this will affect the outcome of the simulation.

The foundation necessary to establish the accuracy of both the computer process and its resulting output generally requires proof of the same matters discussed in connection with the authentication of computer-generated evidence: reliability of the input, processing, and output stages of the process. Because computer-generated evidence is offered through the testimony of a trial expert, underlying data need not be admissible. If the evidence is to be used as demonstrative or illustrative of the opinions of an expert, a proper foundation by the party offering the evidence must be made. Determination of adequacy of the foundation is within the discretion of the trial judge.¹⁴⁴

The law does not recognize UAVs as “persons” and the federal rules of evidence do not apparently reach machine generated speech, however, aviation accident lawyers have used cases involving telephone wire taps as precedent for the proposition that computer-generated records are real evidence and not hearsay evidence contemplated by a traditional business records analysis.¹⁴⁵ The same logic could be applied to UAV-generated evidence. Alternatively, “[i]f admissibility of computer-generated visual evidence cannot be accomplished directly through the relevancy provisions, admission should be sought through the ‘back door’ route of testimony by an expert witness.”¹⁴⁶ And, in any case, although the informational derivatives of drone flights are a relatively new innovation, they are “nothing more than another type of demonstrative evidence whose admissibility requires only that the item be sufficiently explanatory or illustrative of relevant testimony in the case to be of potential help to the trier of fact.”¹⁴⁷

IV. CONCLUSION AND RECOMMENDATIONS

In “There Will Come Soft Rains,” a 1950s short story by Ray Bradbury, readers are introduced to the year 2026 and a post-apocalyptic world in which a computer continues to automate daily housekeeping functions unaware of the fate of the home’s former inhabitants.¹⁴⁸ Representing the sensibilities of a post-war

---

¹⁴⁴. Fadely, supra note 39, at 890-91.
¹⁴⁶. Fadeley, supra note 39, at 868-69 (“Under Federal Rule of Evidence 702, qualified experts provide technical knowledge to assist the trier of fact in understanding the evidence. Furthermore, an expert can base his opinion on facts or data which need not be admissible in evidence if the underlying data are ‘of a type reasonably relied upon by experts in the particular field in forming opinions or inferences upon the subject.’”).
¹⁴⁷. Id. at 827.
¹⁴⁸. See Ray Bradbury, August 2026: There Will Come Soft Rains, COLLIER’S (1950), available at https://docs.google.com/file/d/0BzbtlcAsIeTnTINmSnhOV010bHM/edit?pli=1. The story is based on a 1920s short poem by Sara Teasdale, reading:
generation, this view of a future in which humans destroy themselves is a stark contrast to the dystopian machine-run futures that producers and writers imagine today. Whatever the accuracy of Bradbury’s prediction, his anticipation of a society in which the relationship between humans and machines is intertwined is relatable to modern readers given the advent of automated and fully autonomous flying vehicles.

UAVs are both exciting and worrisome. At one extreme, combat UAVs are among the world’s most effective and lethal warfare machines; at the other extreme, civil UAVs can optimize global commercial networks. In either case, the technology has the capacity to obliterate traditional notions of privacy, trespass, and government searches. But that potentiality should not be met in the first instance by reactionary laws that completely squelch innovation and allowable uses. Many of history’s most significant innovations—airplanes, air conditioning, antibiotics, automobiles, chlorine, the measles vaccine, open-heart surgery, radio, refrigeration, the smallpox vaccine, and X-rays—would have been impossible if met with the restrictive legal environment that lawmakers have built around commercial drones today.¹⁴⁹ Rather than implementing near-sighted laws that, at best, merely slow the latest advance in the digital revolution, lawmakers should accommodate drone operations within the evidentiary and procedural framework that currently exists. Existing Fourth Amendment and privacy protections may be sufficient, though extensive future scholarship on these matters is likely.

For now, there is no question that incorporating UAV operations into the common law and harmonizing the technology’s piercing intelligence and surveillance capabilities with the privacy protections and civil liberties guaranteed under the Constitution are significant challenges for lawmakers. The argument that current practices and procedures may be sufficiently resilient to

There will come soft rains and the smell of the ground,
And swallows circling with their shimmering sound;
And frogs in the pools, singing at night,
And wild plum trees in tremulous white,
Robins will wear their feathery fire,
Whistling their whims on a low fence-wire;
And not one will know of the war, not one
Will care at last when it is done.
Not one would mind, neither bird nor tree,
If mankind perished utterly;
And Spring herself, when she woke at dawn,
Would scarcely know that we were gone.


allow drone-borne technology to evolve further should not be read as minimizing these concerns. But even these lofty challenges should not paralyze lawmakers or the law with respect to the role drone technology can and might play in the courtroom.

A better approach than restricting drone evidence unduly would be to apply the same evidentiary standards to drone forensics as now applies to data and information gained or produced by aerial surveillance generally and other technologies such as cameras, smart phones, and computer-generated visual evidence. Courts could continue to exclude from admission information obtained by drone-deployed technologies deemed violative of common law tort and property rights sounding in privacy and trespass, respectively, as well as Fourth Amendment protections against state searches, e.g., thermal imaging or facial recognition or biometric matching technology. Such an approach would achieve the goal of excluding impermissible drone-acquired evidence from the adjudicative process while otherwise allowing accepted technologies to continue to perform.

In the final analysis, a robust system of legal rules and practices designed to ensure the reliable, resilient, and uncompromised collection and use of UAV data is imperative. And, in many senses, it already exists. Going forward, the development of legal rules and processes in the drone age should not necessarily be more difficult to achieve than formulating laws and policies has historically been with respect to emergent technologies. For as new and cutting edge as drones are and seem, they are not the first new technological innovation to which the law has had to adapt. And, so, while automation is the hallmark of unmanned aviation, reason, logic, and improvisation—hallmarks of the legal system—are the human assets that are most needed as UAV proliferate. Shunning drone-acquired data because it was acquired by drone is not a measured response but rather the result of legislating on the basis of rank anxiety rather than sound policy and empirical evidence.

THE CHANGING EXPECTATION OF PRIVACY: KEEPING UP WITH THE MILLENNIAL GENERATION AND LOOKING TOWARD THE FUTURE

Erin Corken*

ABSTRACT

Data Privacy is the new emerging area of law. Data has been exploding exponentially over the last decade and a half, yet it seems like the legal community along with the rest of the world is just beginning to seriously pay attention to data privacy as the result of related security issues like the many recent data breaches in the retail market within companies like Target, Chic-Fil-A, and Home Depot. We have all been aware of the privacy issues, but they have been on the back burner as we have been too busy running around trying to keep up with all of the emerging technology being created to manage all of the data. We have been telling ourselves that we would get to it later and ignoring that little voice somewhere in the back of our minds that was whispering that we should not put it off. But as lawyers, we are professional procrastinators and we ignored that voice for so long that now many of us are scrambling to get some guidelines together.¹

But, are we wasting our time?

We are living in a new era and as new norms of digital privacy emerge, will we find that there is no longer any expectation of privacy? The new generation of Millennials are exhibitionists compared to the Baby Boomers and even many Generation Xers. Will we spend the next few years of our lives developing ways to make certain that Personal Private Information ("PPI") is protected, only to find that the people we are protecting are openly sharing what we have been trying to protect? Will we find that not only do the Millennials not have an expectation of privacy, but that the world that they envision and will create will

¹ For example, law firms, governments, corporations, and groups like The Sedona Conference. The Sedona Conference’s recently created Working Group 11 focuses on privacy and security issues.
be one of openness, inclusion, and transparency beyond anything we have ever imagined? And, if so, do we have a duty to attempt to steer them in another direction?

This article looks at the history of privacy law, defines “big data,” examines the existence of and derivation of the right to privacy, and explores how the future of privacy law could be affected by the Millennial Generation’s apparently changing attitude.

INTRODUCTION

Privacy law is not new. There are several sources of privacy law in the U.S. and globally. This should be a good thing, right? It is better to have protections in place than not. However, when the protections that are in place are out of date, a false sense of security may exist. After all if no laws were in place it would be obvious that the current state of protection is precarious.²

So, maybe the good thing that is arising out of the recent onslaught of data security breaches is the increased awareness of privacy issues such as outdated privacy regulation, the unprecedented amount of data that is being created exponentially, the confusion and controversy surrounding the right to privacy in general, and changing expectations of what the right to privacy includes.³

This article will examine each of these four areas. In part one, a brief history of data privacy law is presented. Then the major federal statutes in place today that affect data privacy are listed in chronological order, the purpose for each is stated, and what has changed since the laws were first enacted is considered. In part two, how data became “big data” and where it is going is explained. This includes defining several technology related terms and concepts that are essential to know in today’s practice of law. In part three, the existence and derivation of the right to privacy is elucidated. This includes extrapolating from where the right to privacy is derived and identifying the benchmarks for invoking the right. In part four, how the changes that are occurring in society will affect the way future generations view privacy is contemplated, and the question of whether efforts to protect privacy are futile is queried and investigated. Finally, in part five, the article concludes. In the conclusion the question of whether efforts to

². Remarks at the Federal Trade Commission Constitution Center, 2015 DAILY COMP. PRES. DOC. 2 (Jan. 12, 2015) (emphasizing the urgent need for updated data privacy legislation); see also Remarks at the National Cybersecurity Communications Integration Center, 2015 DAILY COMP. PRES. DOC. 3 (Jan. 13, 2015); Address Before a Joint Session of the Congress on the State of the Union, 2015 DAILY COMP. PRES. DOC. 8 (Jan. 20, 2015).
update and create new data privacy law are worthwhile is answered as it depends
on what the future will bring. Likely it will bring more advancement in
technology and having qualified people to manage the technology will be key.

Part I: A brief history of data privacy law
Part II: Defining “big data” terms and concepts
Part III: The existence and derivation of the right to privacy
Part IV: The future of data privacy
Part V: Conclusion

I. A BRIEF HISTORY OF DATA PRIVACY LAW

In the United States under our system of common law, the body of case law
regarding data privacy is constantly changing. Though not developing as
quickly as technology, data privacy litigation has increased significantly in the
past few years and is only expected to continue to increase. There are some
prominent recent federal and state court decisions that will undoubtedly serve as
guides for what is to become the future of modern data privacy case law. The
focus of this article is elsewhere. Rather than trying to summarize the current
body of data privacy case law, this article will instead look at the codification of
privacy law as it exists today. After all, much of the case law being created today
relies upon this body of statutes and regulations for guidance and follows it as
binding or persuasive authority. So, we begin by taking a look at the
development of “modern” federal data privacy statutes.

The origin of modern data privacy law codification begin almost fifty years
ago in the late 1960’s and early 1970’s with the publication of two scholarly
works written by data privacy pioneer Alan Westin, Privacy and Freedom
written in 1970 and Databanks in a Free Society written in 1972. Westin was a
Professor of Public Law & Government Emeritus at Columbia University and
much of the subsequent and “modern” privacy law was based in large part on his

   2015/.
5. See id.
   Cir. 2012); see also Zurich Am. Ins. v. Sony Corp. of Am., No. 651982/2011, 2014 WL 3253541
7. See Bateman v. American Multi-Cinema, Inc., 623 F.3d 708, 710 (9th Cir. 2010) (class
   certification denied under FACTA); see also Torres v. Nutrisystem, Inc., 289 F.R.D. 587, 590
   (C.D. Cal. 2013) (class certification denied under CIPA).
8. See Margalit Fox, Alan F. Westin, Who Transformed Privacy Debate Before the Web Era,
   Emily Langer, Alan F. Westin, Scholar of Privacy in the Information Ages, Dies at 83, WASH. POST
   information-ages-dies-at-83/2013/02/19/7258b28c-7aa6-11e2-a044-676856536b40_story.html.
books and research. This included several government reports that followed shortly after Westin’s seminal works were published, such as the 1973 U.S. Secretary of Health, Education, and Welfare Advisory Committee on Automated Personal Data Systems report, Records, Computers and the Rights of Citizens that set out a code of fair information practice that included principles that would become known as fair information practice principles (“FIPPs”). The original four principles were (1) Notice; (2) Choice; (3) Access; and (4) Security.

The Notice principle was also known as the awareness or collection principle, and it stated that consumers should be given notice before any information is collected from them. The Choice principle was also known as the consent principle, and it stated that consumers should be given the choice of whether to “opt-in” or “opt-out” of the use of their information. The Access principle was also known as the participation principle, and it stated that consumers should be able to view and verify the accuracy of the information collected. The Security principle was also known as the integrity principle, and it stated that those collecting information should ensure that collected data is accurate and secure.

These first FIPPs served as the basis for the next major development in modern privacy law, the Privacy Protection Act of 1974 (“PPA”). The PPA was one of the first pieces of legislation enacted specifically to regulate personal information. It was enacted to regulate the Federal Government’s collection, maintenance, use, and dissemination of personal information in systems of records.

Many other laws enacted before or after, like the Fair Credit Reporting Act (“FCRA”) enacted in 1970 and the Fair Debt Collection Practices Act of 1977 (“FDCPA”), have provisions with major implications regarding personal information and data privacy. However, they were enacted to regulate specific
things other than data privacy such as the collection, dissemination, and use of consumer information, including consumer credit information in the case of the FCRA and consumer credit rights in the case of the FDCPA.\footnote{See Peter P. Swire & Keesha Ahmad, Foundations of Information Privacy and Data Protection: A Survey of Global Concepts, Laws and Practices 71-73 (2012).} The PPA was the first piece of U.S. federal legislation with the specific purpose of regulating the privacy of personal information.\footnote{See id. at 70.}


The next major development in data privacy regulation occurred in Europe in 1980 when the Organization for Economic Cooperation and Development (“OECD”) expanded on the original four FIPPs and adopted a more comprehensive version of eight principles.\footnote{OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, Org. Econ. Co-Operation & Dev. [hereinafter OECD Guidelines], http://www.oecd.org/internet/ieconomy/oecdguidelinesonthe protecionofprivacyandtransborderflowsopersonaldata.htm (see “Part Two”).} The OECD eight FIPPs, along with the Council of Europe’s Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data and the European Union Data Protection Directive, form the basis of the majority of European data privacy law that exists today.\footnote{Id. There is a new law that has been proposed by the European Commission that will unify data protection into a single law, the General Data Protection Regulation. The proposed law includes a right to erasure that allows an individual to ask that his personal information be deleted on any one of a number of grounds. This is similar to but offers less protection than the “right to be forgotten” which was recently recognized in a European Union Court of Justice decision, Google Spain SL and Google Inc. v. Agencia Espanola de Proteccion de Datos (APED) and Mario Costeja Gonzalez (C-131-12).}

The comprehensive OECD FIPPs include (1) The Collection Limitation Principle; (2) The Data Quality Principle; (3) The Purpose Specification Principle; (4) The Use Limitation Principle; (5) The Security Safeguards Principle; (6) The Openness Principle; (7) The Individual Participation Principle; and (8) The Accountability Principle.\footnote{Id.}

The Collection Limitation Principle is a combination of the original Notice and Choice principles. It states that consumers should have knowledge of and consent to the data subject being collected, where appropriate.\footnote{Id.} It is broader
than both the Notice and Choice principles and it states that there should be limits to the amount of data collected and that data should be collected by lawful and fair means.\textsuperscript{27}

The Data Quality Principle states that collected data should be relevant to the purposes for which it will be used, and similar to the original Security principle, it states that the collected data should be accurate, complete, and kept up-to-date.\textsuperscript{28}

The Purpose Specification Principle is another principle similar to the original Notice principle. In addition to simply giving notice that information is being collected it states that the specific purposes for which personal data is collected should be specified at the time of data collection, and that the subsequent use should be limited to the fulfillment of the specified or compatible purposes.\textsuperscript{29}

The Use Limitation Principle is similar to the original Security principle and states that personal data should not be disclosed, made available, or otherwise used for purposes other than those specified in accordance with the specified purposes unless there is consent or legal authority.\textsuperscript{30}

The Security Safeguards Principle also like the original Security principle states that personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification, or disclosure of data.\textsuperscript{31}

The Openness Principle is a broader more comprehensive version of the original Access principle. It states that those collecting data need to do more than merely make the collected data available to the consumer to be verified.\textsuperscript{32} In addition, there should be a general policy of openness about developments, practices, and policies with respect to personal data.\textsuperscript{33} Also, means should be readily available to establish the existence and nature of personal data, the main purposes of their use, as well as the identity and usual residence of the data controller.\textsuperscript{34}

The Individual Participation Principle, also similar to the original Access principle, states that an individual should have various specified rights regarding access to and verification of data.\textsuperscript{35}

The Accountability Principle states that a data controller should be accountable for complying with measures which give effect to the principles.\textsuperscript{36}

\textsuperscript{27} Id.
\textsuperscript{28} Id.
\textsuperscript{29} OECD Guidelines, supra note 23, Part II.
\textsuperscript{30} Id.
\textsuperscript{31} Id.
\textsuperscript{32} See id.
\textsuperscript{33} Id.
\textsuperscript{34} Id.
\textsuperscript{35} See OECD Guidelines, supra note 23, Part II.
\textsuperscript{36} Id.
This principle is similar to and likely the basis of the subsequent original fifth U.S. FIPP, Enforceability.

In 1998, the Federal Trade Commission (“FTC”) issued a report that added a fifth principle, the Enforcement principle, also known as the redress principle which identified three types of enforcement: (1) self-regulation; (2) private remedies; and (3) government enforcement.\(^{37}\) For the next ten years, the U.S. seemingly relied upon the five FIPPS, the original four and the Enforcement principle, rather than adopting the more extensive eight European principles. It was not until 2008, when the Department of Homeland Security (“DHS”) announced they would begin following an expanded version of the FIPPs which included eight principles similar to the OECD principles.\(^{38}\) The National Institute of Standards and Technology (“NIST”) initiative and The National Strategy for Trusted Identities in Cyberspace (“NSTIC”) lists the expanded eight principles as well.\(^{39}\)

The eight U.S. FIPPS are (1) Transparency (similar to the original Notice and the OECD Openness); (2) Individual Participation (similar to the original Access, Choice, and Enforcement); (3) Purpose Specification (similar to the OECD Individual Participation, but it also states that the data collectors should state the authority that permits collection); (4) Data Minimization (similar to the OECD Collection Limitation, but it also states that data should only be kept for as long as necessary to fulfill the specified purpose); (5) Use Limitation (similar to the OECD Use Limitation); (6) Data Quality and Integrity (similar to the original Security and the OECD Data Quality); (7) Security (similar to the OECD Security); and (8) Accountability and Auditing, which requires self-regulation.\(^{40}\)

The chart below compares the expanded more comprehensive eight FIPPS as used in the U.S. with the OECD eight FIPPS. It also shows the overlap between both sets of expanded FIPPs and the original four FIPPs.

---


40. See DHS, supra note 35; see also National, supra note 16.
In 2012, the Obama Administration proposed a Consumer Privacy Bill of Rights ("CPBR") based upon and very similar to the OECD/DHS-NSTIC FIPPs.\(^{41}\) The CPBR includes only seven principles: (1) Respect for Context (similar to Collection Limitization/Data Minimization); (2) Focused Collection (similar to Collection Limitization/Data Minimization); (3) Security (similar to Security); (4) Accountability (similar to Accountability/self-regulation); (5) Individual Control (similar to Individual Participation); (6) Transparency (similar to Openness/Transparency); and (7) Access and Accuracy (similar to Openness/Transparency and Security).\(^{42}\)

Over the years in the U.S., following the FIPPs as the primary source of guidance for the most part, a sectoral approach to privacy regulation has developed. Rather than one comprehensive statute regarding data privacy or several pieces of legislation specifically focusing on the privacy of personal information, much of the legislation in the U.S. regulates other areas such as consumer protection, records management in federal agencies, telecommunications, electronic communication, healthcare, banking and financial institutions, education, audio visual material rental, sale and subscription, electronic government services, children, and drivers that typically concern provisions regarding personal information and the safeguarding of it. Very little legislation exists specifically to regulate data privacy.\(^{43}\)


\(^{42}\) See id.

\(^{43}\) See generally Swire & Ahmad, supra note 19, at 67-76.
To illustrate U.S. sectoral approach to data privacy legislation, here is a brief chronological list of the more common U.S. federal statutes with significant provisions regarding data privacy. The following descriptions are of the statutes as originally enacted.\textsuperscript{44}

**Federal Trade Commission Act of 1914 (“FTCA”)\textsuperscript{45}**

**Area:** Consumer Protection

**Purpose:** To establish the FTC to issue “cease and desist” orders to large corporations to curb unfair trade practices.\textsuperscript{46} Section 5 of the Act declares that unfair or deceptive acts or practices (“UDAPs”) affecting commerce are illegal.\textsuperscript{47}

**What has changed:** Since the enactment of the FTCA in 1914, the way the entire world conducts business has changed. With the invention of the Internet, we now live in a global economy where consumer transactions take place instantaneously. For example, Amazon.com was launched in 1994.\textsuperscript{48} E-Bay was launched in 1995.\textsuperscript{49}

**Federal Records Act of 1950 (“FRA”)\textsuperscript{50}**

**Area:** Records Management in Federal Agencies

**Purpose:** To regulate federal agency record keeping.\textsuperscript{51}

**What has changed:** It was not until 1971 that email was invented.\textsuperscript{52}

\textsuperscript{44} Of course over time many of the laws have been amended and the reach of the statutes have changed. Yet, many of the changes are not related to data privacy, and the changes that are related to data privacy are generally inadequate or outdated.


\textsuperscript{46} 15 U.S.C. § 45(b) (2014).


\textsuperscript{49} Erica Swallow, *10 Entertaining eBay Facts You Might Not Know*, MASHABLE (Aug. 7, 2010, 2:09 PM), http://mashable.com/2010/08/07/ebay-facts/. Additionally, sound film, television, rocketry, the jet engine, the ballpoint pen, Teflon, color television, the photocopier, nuclear fission, the helicopter, the atomic bomb, relay satellites, transistors, and penicillin were all invented after the enactment of the FTCA. James Fallows, *The 50 Greatest Breakthroughs Since the Wheel*, ATLANTIC, (Oct. 23, 2013, 7:08 PM), http://www.theatlantic.com/magazine/archive/2013/11/innovations-list/309536/.

\textsuperscript{50} 44 U.S.C. §§ 3101-07 (2014).


\textsuperscript{52} Mary Bellis, *History of Email & Ray Tomlinson*, ABOUT.COM, http://inventors.about.com/od/estartinventions/a/email.htm (last visited Apr. 4, 2015). Also, the first man in space and the Moon landing happened after the FRA was enacted. See Fallows, supra note 50. Further, women like my mother stopped curling their hair with beer cans. The electric curling iron was invented in 1959. See *When was the Curling Iron Invented?*, WHENWASITINVENTED.ORG, http://www.whenwasinvented.org/when-was-the-curling-iron-invented/ (last visited Apr. 4, 2015). The FDA approved the birth control pill in 1957. See
Bank Secrecy Act of 1970\textsuperscript{53}

Area: Financial Institution Record Keeping and Reporting

Purpose: To require financial institutions to assist government agencies to detect and prevent money laundering.\textsuperscript{54} It imposes extensive record keeping and reporting requirements.\textsuperscript{55}

What has changed: The pocket calculator was invented in 1971\textsuperscript{56} and the personal computer was invented in 1975.\textsuperscript{57}

Fair Credit Reporting Act of 1970 ("FCRA")\textsuperscript{58}

Area: Consumer Credit

Purpose: To protect personal financial information regarding consumer credit.\textsuperscript{59} To promote accuracy, fairness, and privacy protection with regard to the information assembled by consumer reporting agencies.\textsuperscript{60}

What has changed: The first cell phone did not exist until 1973.\textsuperscript{61} Microsoft Office 1.0 was released in 1990.\textsuperscript{62}

\hspace{1cm} Suzanne White Junod, \textit{FDA’s Approval of the First Oral Contraceptive, Enovid, FOOD & DRUG LAW INST.}, http://www.fda.gov/AboutFDA/WhatWeDo/History/ProductRegulation/SelectionsFromFDLIUpdateSeriesonFDAHistory/ucm092009.htm (last updated Apr. 15, 2009).
\hspace{1cm} 53. 31 U.S.C. §§ 5311 – 5330 (2014).
\hspace{1cm} 55. See id.; see also 31 C.F.R. § 1010.310 (2014).
\hspace{1cm} 57. See \textit{INVENTION OF THE PC, HISTORY}, http://www.history.com/topics/inventions/invention-of-the-pc (last visited Apr. 4, 2015).
\hspace{1cm} 58. 15 U.S.C. §§ 1681 – 1681x (2014) (amended in 1996 by the Consumer Credit Reporting Reform Act; and in 2003 by the Fair and Accurate Credit Transactions Act (FACT Act)).
\hspace{1cm} 60. Id.
Privacy Act of 1974\textsuperscript{63}

\textbf{Area:} Personal Information in Federal Government Records

\textbf{Purpose:} To regulate the federal government’s maintenance, collection, use, and dissemination of personal information in systems of records.\textsuperscript{64}

\textbf{What has changed:} The first Apple computer was released in 1976.\textsuperscript{65}

Family Educational Rights and Privacy Act of 1974 (“FERPA”)\textsuperscript{66}

\textbf{Area:} Education

\textbf{Purpose:} To protect the privacy of educational records.\textsuperscript{67}

\textbf{What has changed:} The Sony Walkman, CD-ROMS, and Personal Data Assistants (PDAs) were all invented after 1974, and they all are virtually obsolete now.\textsuperscript{68}

Fair Debt Collection Practices Act of 1977 (“FDCPA”)\textsuperscript{69}

\textbf{Area:} Consumer Credit

\textbf{Purpose:} To protect consumers from abusive debt collection practices.\textsuperscript{70}

\textbf{What has changed:} Flash memory was not around until 1984 and Windows was invented in 1985.\textsuperscript{71}

Protection of Pupil Rights Amendments of 1978 (“PPRA”)\textsuperscript{72}

\textbf{Area:} Education

\begin{footnotesize}
\begin{itemize}
\item 63. 5 U.S.C. § 552a (2014).
\item 64. Id.
\item 66. 20 U.S.C. § 1232g (2014).
\item 67. See id.
\item 70. 15 U.S.C. § 1692(e) (2014).
\item 71. EDWIN D. REILEY, \textit{MILESTONES IN COMPUTER SCIENCE AND INFORMATION TECHNOLOGY} 348 (2003).
\item 72. 20 U.S.C. § 1232h (2014).
\end{itemize}
\end{footnotesize}
Purpose: To regulate collected student information. 73

What has changed: The camcorder was not around before 1983,74 not to mention YouTube, Snapchat, Twitter, and even Facebook.75

Computer Fraud and Abuse Act of 1986 (“CFAA”)76
Area: Electronic Communications

Purpose: To criminalize the access of protected computer information.77

What has changed: Portable Data Files (PDFs) were not around until 199378 and Joint Photographic Expert Group files, also known as JPEGs, were not around until 1987.79

Electronic Communications Privacy Act of 1986 (“ECPA”)80
Area: Electronic Communications

Purpose: To extend government restrictions on wire taps from telephone calls to include transmissions of electronic data by computer.81

Stored Communications Act of 1986 (“SCA”)82
Area: Electronic Communications

Purpose: Title II of the ECPA. To regulate the electronic communications of Internet Service Providers (“ISPs”).83

What has changed: Although technically the Internet existed prior to 1986, the World Wide Web was not invented until 1989.84

73. See id.
76. 18 U.S.C § 1030 (2014).
77. Id.
Video Privacy Protection Act of 1988 (“VPPA”)\(^{85}\)

**Area:** Audio Visual Material Rental, Sale and Subscription

**Purpose:** To prevent wrongful disclosure of video tape rental, sale, or subscription information.\(^{86}\)

**What has changed:** Netflix was not in business until 1997.\(^{87}\) Blockbuster had physical stores.\(^{88}\) Redbox was not around before 2002.\(^{89}\)

Telephone Consumer Protection Act of 1991 (“TCPA”)\(^{90}\)

**Area:** Telecommunications

**Purpose:** To amend the Communications Act of 1934, and to regulate telemarketing and the use of automated dialing systems.\(^{91}\)

**What has changed:** Text messaging did not begin until 1992.\(^{92}\) Personal GPS devices were not around before 1993.\(^{93}\) Broadband first started being used in 1995 enabling hi-speed internet connections.\(^{94}\) Anyone remember dial up and AOL? “You’ve got mail.”

Driver’s Privacy Protection Act of 1994 (“DPPA”)\(^{95}\)

**Area:** Drivers

---

86. See id.
Purpose: To regulate the privacy and disclosure of personal information gathered by state Departments of Motor Vehicles.\textsuperscript{96} Applies to Departments of Motor Vehicles as well as other recipients of personal information.\textsuperscript{97}

What has changed: Global Positioning System ("GPS") navigation devices in most automobiles now collect information regarding vehicle location.\textsuperscript{98}

Telecommunications Act of 1996\textsuperscript{99}

Area: Telecommunications

Purpose: To amend the Communications Act of 1934.\textsuperscript{100} It was the first time that the Internet was included in broadcasting and spectrum allotment.\textsuperscript{101}

What has changed: The iPhone was first released in 2007.\textsuperscript{102} The widespread use of other smartphone devices was also subsequent to the enactment of the Telecommunications Act.\textsuperscript{103} The number of smart phones being used reached one billion in 2012.\textsuperscript{104} It took fourteen years to reach that number and is expected to reach two billion by 2015.\textsuperscript{105}

Clinger-Cohen Act of 1996 ("CCA") (formerly known as the Information Technology Management Reform Act) ("ITMRA")\textsuperscript{106}

Area: Information Technology

Purpose: To improve the way the federal government acquires, uses, and disposes information technology.\textsuperscript{107}

\textsuperscript{96} 18 U.S.C. § 2721 (2014).
\textsuperscript{97} See 18 U.S.C. § 2721(c) (2014).
\textsuperscript{100} See id.
\textsuperscript{101} See id.
\textsuperscript{104} See id.
\textsuperscript{105} See id.
What has changed: It was not until 2000 that sixty percent of U.S. households had at least one computer. 108

Health Insurance Portability and Accountability Act of 1996 ("HIPAA") 109

Area: Healthcare

Purpose: To regulate the use and disclosure of individual health information by specified covered entities. 110

What has changed: Google did not exist until 1998, enough said. 111

Children’s Online Privacy Protection Act of 1998 ("COPPA") 112

Area: Children and Personal Information

Purpose: To regulate the online collection of personal information from children. 113

What has changed: Blackberries (not the fruit) were first released in 1999. 114 Even more shocking is that Wikipedia did not exist yet. It was launched in 2001 as well. 115 The iPod did not exist until 2001. 116 Amazon Kindle and other e-reading devices were not prevalent until 2007. 117

Gramm-Leach-Bliley Act ("GLB") / Financial Services Modernization Act of 1999 118

Area: Banks and Financial Institutions

Purpose: To establish guidelines for the protection of personal financial information. 119 It requires financial institutions to provide a privacy policy to customers, which explains what kinds of information are being collected and how

---

108. See Ball, supra note 83.
111. See Ball, supra note 83.
115. Id.
116. See Ball, supra note 83.
117. See Woodford, supra note 93.
that information is used, and to develop safeguards in order to protect the information they collect from customers.\footnote{120. See 15 U.S.C. § 6802 (2014).}

**What has changed:** File sharing was developed in 2001, two years after the enactment of the GLB Act.\footnote{121. See Woodford, supra note 93.}


**Area:** Electronic Government Services

**Purpose:** To improve the management and promotion of electronic government services and processes by establishing a Federal Chief Information Officer within the Office of Management and Budget, and by establishing a framework of measures that require using Internet-based information technology to improve citizen access to government information and services, and for other purposes.\footnote{123. Pub. L. No. 107-347, 116 Stat. 2962 (2002).}

**What has changed:** Text messaging was available prior to 2003, but Wi-Fi was not common until that year.\footnote{124. See Ball, supra note 83.}


**Area:** Personal Information

**Purpose:** Title III of the E-Government Act. It requires federal agencies to have information security programs for information and information systems that support the operations and assets of the agency.\footnote{126. See 44 U.S.C. § 3551 (2014).}


**Area:** Personal Information

**Purpose:** Title V of the E-Government Act. It establishes uniform confidentiality protections for information collected for statistical purposes by U.S. statistical agencies.\footnote{128. See 44 U.S.C. § 3501 (2014).}

**What has changed:** CIPSEA was enacted prior to the release of the iPad. It is hard to believe that tablet devices have only been around since 2010.\footnote{129. See 44 U.S.C. § 3501 (2014).}
Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (“CAN-SPAM”)\(^\text{130}\)

**Area:** Electronic Communications

**Purpose:** To establish national standards for sending commercial e-mail.\(^\text{131}\)

**What has changed:** Since 2003 when the CAN SPAM Act was enacted, many important technological advancements regarding electronic communications have occurred, such as the start of cloud computing and GoogleDocs (now Google Drive)\(^\text{132}\).

II. DEFINING “BIG DATA” TERMS AND CONCEPTS

Data has been around for centuries. From prehistoric cave paintings dating back 40,000 years\(^\text{133}\) and through the development of civilization, the amount of data in existence has seemingly expanded at a rather rapid pace.\(^\text{134}\) From clay tablets used for the first books in Mesopotamia through the invention of papyrus, parchment, and the printing press;\(^\text{135}\) with each new development in the history of writing, data has been expanding.

Eventually, with additional technological developments data came to include other types of information such as photographs and audio and visual recordings. These types of information were in hard copy form at first. Then with the proliferation of computers and computer technology a shift began to occur to where the form of the majority of data being created turned from hard copy to electronic. The product of this shift, the data created electronically whether electronic written documents, electronic audio, and visual recordings, or other types of electronic information is what is considered “big data.”\(^\text{136}\)

When we refer to the rate at which the amount of data in existence is increasing, we usually say it is increasing exponentially, which means that it is increasing proportionally to the rate at which technology is advancing. However,

---

\(^{129}\) See Woodford, *supra* note 93.


\(^{132}\) See *Google Announces Limited Test on Google Labs: Google Spreadsheets, Google* (June 6, 2006), http://googlepress.blogspot.com/2006/06/google-announces-limited-test-on-

\(^{133}\) Helen Thompson, *Rock (Art) of Ages: Indonesian Cave Paintings Are 40,000 Years Old*, *Smithsonian* (Oct. 8, 2014), http://www.smithsonianmag.com/science-nature/


\(^{135}\) See *Early Writing*, *The Univ. of Tex. at Austin*, http://www.hrc.utexas.edu/educator/modules/gutenberg/books/early/ (last visited Apr. 5, 2015).

\(^{136}\) See *Executive Office of the President, supra* note 144, at 1-4.
it was not until recently that the definition of “exponentially” took on an entirely new meaning. Before “big data,” spanning from the dawn of civilization to 2003, five exabytes of data were created.\(^{137}\) Today, over five exabytes of data are created in less than two days, and the amount of data being created is still increasing.\(^{138}\)

So, how much data is five exabytes? There are a couple of ways to look at it for perspective. A typical hard drive size is 320 gigabytes (“GBs”) to 500 GBs.\(^{139}\) One GB is approximately 64,000 pages in Microsoft® Word® or 100,000 emails depending on the amount of information on each page or in each email.\(^{140}\)

A gigabyte is a thousand megabytes which is represented numerically as the digit one with three zeros following it (1,000).\(^{141}\) It used to be when we talked about data amounts, speaking in terms of gigabytes was enough. Now we have to move up the metric scale to terabytes, petabytes, exabytes, zettabytes, and yottabytes.

A terabyte (“TB”) is one thousand gigabytes or the digit one with 12 zeros following it, (1,000,000,000,000).\(^{142}\) A petabyte (“PB”) is one million gigabytes or the digit one with 15 zeros following it, (1,000,000,000,000,000).\(^{143}\) An Exabyte (“EB”) is a billion gigabytes or the digit one with 18 zeros following it, (1,000,000,000,000,000,000).\(^{144}\) A zettabyte (“ZB”) is one trillion gigabytes or the digit one with 21 zeros following it, (1,000,000,000,000,000,000,000).\(^{145}\) A yottabyte (“YB”) is one quadrillion gigabytes or the digit one with 24 zeros following it, (1,000,000,000,000,000,000,000,000).\(^{146}\)

An easy way to remember this progression of bytes is with the mnemonic phrase “tooth paste erases zero yellow,” where the first letter of each word in the phrase represents the next level of the metric scale starting with “t” for tera, “p” for peta, “e” for exa, “z” for zetta, and “y” for yotta. Another way to look at it for perspective is to consider that by 2012, it was estimated that the digital universe of data was to have grown to 2.72 zettabytes, and that it would at least

---


\(^{138}\) Id.


\(^{142}\) See id.

\(^{143}\) See id.

\(^{144}\) See id.

\(^{145}\) See id.

\(^{146}\) See id.
double every two years to reach 8 zettabytes by 2015.\textsuperscript{147} That’s the equivalent of 18 million Libraries of Congress.\textsuperscript{148}

Billions of connected devices, ranging from personal computers (“PCs”) and smart phones to sensor devices such as RFID readers and traffic cams, generate this flood of Electronically Stored Information (“ESI”) that includes both structured data and unstructured data.\textsuperscript{149} “Structured data” is data that is organized in some formal way such as data from a database.\textsuperscript{150} “Unstructured data” is data that is not formally organized.\textsuperscript{151} It accounts for the majority of data created and includes e-mail and word processing documents such as those created from Microsoft Word, spreadsheets like Excel documents, presentations such as Power Points, image documents such as .jpegs and .gifs, audio files such as MP3s, video files such as MP4s,.pdfs, and etc.\textsuperscript{152} Computer World states that unstructured information might account for more than seventy to eighty percent of all data in organizations, and multiple analysts have estimated that the total amount of both structured and unstructured data will grow eight-hundred percent over the next few years.\textsuperscript{153}

\section*{III. The Existence and Derivation of the Right to Privacy}

When we talk about privacy, the first thing we must do is distinguish between the right to privacy in general and data privacy. The right to privacy in general is a fundamental human right.\textsuperscript{154} Data privacy is derived from this fundamental right. As noted above, the first scholarly works that led to modern data privacy law in the United States appeared almost fifty years ago with Westin’s seminal works.\textsuperscript{155} The first significant scholarly work regarding the right to privacy in general is usually credited as occurring much early with

\begin{itemize}
\item\textsuperscript{147} See Gartner, supra note 147.
\item\textsuperscript{150} See The SEDONA CONFERENCE, supra note 159, at 42.
\item\textsuperscript{151} See id. at 48.
\item\textsuperscript{152} See id.
\item\textsuperscript{155} See ALAN F. WESTIN, PRIVACY AND FREEDOM (1970); ALAN F. WESTIN & MICHAEL A. BAKER, DATABANKS IN A FREE SOCIETY: COMPUTERS, RECORD-KEEPING AND PRIVACY (1972).
\end{itemize}
Samuel Warren’s and Louis Brandeis’ 1890 Harvard Law Review article, *The Right to Privacy*.156 In *The Right to Privacy*, Warren and Brandeis discuss how the common law at the time had already began to recognize that privacy was something that required due protection.157 They quote Judge Cooley from his 1878 publication, *A Treatise on the Law of Torts or the Wrongs Which Arise Independently of Contract*, describing it as “the right to be let alone.”158

Ironically, Warren’s and Brandeis’ article was written in response to new technological developments at the time, the instantaneous photograph and newspaper enterprise, which they argued, “have invaded the sacred precincts of private and domestic life.”159 They go on to say that, “numerous mechanical devices threaten to make good the prediction that ‘what is whispered in the closet shall be proclaimed from the house-tops.’”160 This prescient work is widely regarded as spurring the doctrine regarding the tort of invasion of privacy.161

The common law of torts is just one of the many sources to look at as evidence of the existence of the right to privacy.162 In the United States for many years, it has been necessary to look for sources of evidence from which the right to privacy is derived, as the right it is not expressed anywhere in the Constitution.163 Since other rights are specifically enumerated, such as freedom of speech, press, and religion, the right to bear arms, etc… in the Bill of Rights, some strict constructionists have argued that there is not a right to privacy.164 They posit that since so many specific rights are listed had the authors of the Constitution intended for it to include the right to privacy, they would have specifically mentioned it.165

The counterargument has always been that the Ninth and Tenth Amendments specifically retain rights not expressly listed to the people.166 The authors of the

156. See, e.g., Dorothy J. Glancy, *The Invention of the Right to Privacy*, 21 ARIZ. L. REV. 1, 1 (1979) (“The right to privacy is, as a legal concept, a fairly recent invention. It dates back to a law review article published in December of 1890 by two young Boston lawyers, Samuel Warren and Louis Brandeis.”).


158. Id. at 195.

159. Id.

160. Id.


162. See RESTATEMENT (SECOND) OF TORTS § 652A (1977) (noting that the tort of Invasion of Privacy includes four causes of action: Intrusion of Solitude; Public Disclosure of Private Facts; False Light; and Appropriation).

163. The Penumbral Theory as first expressed in *Griswold v. Connecticut*, 381 U.S. 479 (1965), recognized that even though a right to privacy is not expressed or mentioned in the U.S. Constitution, it can be found in the penumbras of other constitutional protections in the Bill of Rights.


165. See id.

166. See id.
Constitution recognized that it would be impossible to list every right they intended to be included, so they created two “catch all” provisions in the Ninth and Tenth Amendments that provide, “[t]he enumeration in the Constitution, of certain rights, shall not be construed to deny or disparage others retained by the people,” and “[t]he powers not delegated to the United States by the Constitution, nor prohibited by it to the states, are reserved to the states respectively, or to the people,” respectively.167 Other amendments that have been recognized as providing additional evidence in support of the existence of the right to privacy include the First Amendment, the Third Amendment, the Fifth Amendment, and the Fourteenth Amendment.168

The First Amendment is the basis for privacy of beliefs.169 It states, “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.”170

The Third Amendment is the basis for privacy of the home.171 It states, “[n]o soldier shall, in time of peace be quartered in any house, without the consent of the owner, nor in time of war, but in a manner to be prescribed by law.”172

The Fourth Amendment is the basis for privacy of the person and possessions.173 It states,

“[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.”174

The Fifth Amendment is the basis for privacy of the innermost sanctity of a person’s mind from compulsory government intrusion.175 It provides that people have the right to keep information about themselves private;

“[n]o person shall be held to answer for a capital, or otherwise infamous crime, unless on a presentment or indictment of a Grand Jury, except in cases arising in the land or naval forces, or in the Militia, when in actual service in time of War or public danger; nor shall any person be subject for the same offense to be twice put in jeopardy of
life or limb; nor shall be compelled in any criminal case to be a witness against himself, nor be deprived of life, liberty, or property, without due process of law; nor shall private property be taken for public use, without just compensation.” 176

The Fourteenth Amendment provides a substantive due process right to privacy:

“[n]o state shall make or enforce any law which shall abridge the privileges or immunities of citizens of the United States; nor shall any state deprive any person of life, liberty, or property, without due process of law; nor deny to any person within its jurisdiction the equal protection of the laws.” 177

The Supreme Court has in several decisions recognized the language regarding due process of law as providing a substantive due process right to privacy. 178

Internationally, the existence of the right to privacy has been much less controversial. The United Nations Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights and many other international and regional treaties all expressly recognize the right to privacy as a fundamental human right. 179 Article 12 of the 1948 Universal Declaration of Human Rights, specifically states, “[n]o one should be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks on his honour or reputation. Everyone has the right to the protection of the law against such interferences or attacks.” 180

Now that we know the sources of the right to privacy, what is the benchmark for determining when the right can be invoked? In the U.S., in both civil and criminal law, the main benchmark seems to be whether there is a reasonable expectation of privacy. 181 This expectation should be objectively rather than subjectively reasonable in that it should include legitimate expectations of

---

176. U.S. CONST. amend. V.
178. See Clark, supra note 178, at 847.
179. Banisar & Davis, supra note 164.
181. Intrusion Upon Seclusion, one of the four invasion of privacy causes of action, is applicable to a reasonableness standard. See supra note 172. “[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.” RESTATEMENT (SECOND) OF TORTS § 652B (1977); see also EXECUTIVE OFFICE OF THE PRESIDENT, supra note 144 (providing Katz v. United States, 389 U.S. 347, 361 (1967) overturned Olmstead v. United States, 277 U.S. 438 (1928)) (“In Katz, the Court held that the FBI’s placement of a recording device on the outside of a public telephone booth without a warrant qualified as a search that violated the ‘reasonable expectation of privacy’ of the person using the booth, even though the device did not physically penetrate the booth, his person, or his property. Under Katz, an individual’s subjective expectations of privacy are protected when society regards them as reasonable.”).
privacy generally recognized by society rather than an individual’s personal opinion or beliefs regarding expectations of privacy.

In civil law, reasonableness is determined by looking to the legal construct of a reasonable person. This construct is explained as not a typical person, but rather a typical member of the community. The adjudicator of fact is to assume the place of a typical member of the community when determining whether an action would be considered reasonable.

In very broad terms, in criminal law, under the Fourth Amendment courts have found that it is reasonable for people to have expectations of privacy in their residences, hotel rooms, and public restrooms. However, people cannot have reasonable expectations of privacy in things held out to the public, such as garbage left for collection in a public place, anything in open fields, and what is observed pursuant to aerial surveillance that is conducted in public navigable airspace.

So, if it is not reasonable to have an expectation of privacy in things held out to the public, such as things in open fields or things that can be observed from the air, is it reasonable to have an expectation of privacy in things held out to the public on the Internet or things that can be observed in the cloud? Further, if the legal construct of a reasonable person today would consider it reasonable, will the legal construct of a reasonable person of tomorrow consider it reasonable?

IV. THE FUTURE OF DATA PRIVACY

The Millennial Generation is defined as the generation following Generation X. The Millennials include people born anywhere from the 1980s to the 2000s. As we have seen above when looking at all the changes since the enactment of much of the legislation affecting data privacy, this generation has grown up in a world where openness, inclusion, and transparency are the norm.

For those of us born before 1980, before camcorders, smart phones, and the Internet, it is reasonable to expect that if someone takes our picture we could stop them from publishing it somewhere without our knowledge. It is reasonable to expect that our picture is not being taken without our knowledge. I can

183. See id.
184. See id.
188. See id.
189. See supra Part I.
remember from my early years working in television prior to law school, and having to obtain releases signed by anyone who might be in a shot on a production.

Further, it is reasonable to expect that we are not being photographed twenty-four hours a day and seven days a week without our knowledge like a character in Orwell’s novel, but we are.\textsuperscript{190} A friend of mine had a break in a year or so ago, and although she did not have a security surveillance device set up at her house, her neighbor across the street had one in his home and the angle of the camera was wide enough to include her front porch. The Home Owners Association (“HOA”) in the community where I live has video surveillance of all the common places in the community recording everything twenty-four hours a day, seven days a week, and they are considering putting cameras in additional areas angled in such a way to capture the entire community. Again, for many of us this seems shocking and wrong. But, for people who are being born into today’s world, it is the norm. Is it reasonable for us to expect them to value something they have never had? Do we have a duty to protect this evanescent right for them? If so, to what extent and why?

President Obama, born in 1961,\textsuperscript{191} thinks we do have a duty to protect privacy. Upon the release of the Consumer Privacy Bill of Rights, he said “[e]ven though we live in a world in which we share personal information more freely than in the past, we must reject the conclusion that privacy is an outmoded value…. [Privacy] has been at the heart of our democracy from its inception, and we need it now more than ever.”\textsuperscript{192}

President Obama may be right. According to his administration’s public survey that was part of the recent 90-Day Review of Big Data and privacy, where they asked people to tell them how concerned they are with various data practices and how much they trust various institutions to keep their data safe and handle it responsibly, respondents felt most strongly about data use and collection practices, expressing a great deal of concern about all of the practices described in the survey.\textsuperscript{193} The ages of the respondents were not included in the online findings.\textsuperscript{194} Further, a recent informal survey, where a group of young engineers were polled, found that the engineers vigorously objected to the government or

\begin{itemize}
  \item \textsuperscript{194} See id.
\end{itemize}
their employers collecting information they had posted on social media. And if you ask my little sister who was born in 1991 and recently had her identity stolen, she would likely agree with the engineers and the Obama administration.

Yet, there are conflicting studies. A recent NPR-Truven Health Analytics Health Poll found that regarding medical data privacy, people were not that concerned about what happens to their information. This same sentiment was expressed years ago by Sun Microsystems founder Scott McNealy, who in 1999 said that privacy issues were “a red herring ...[because] [y]ou have zero privacy anyway. Get over it.”

Is Mr. McNealy right? Are we wasting our time? Do we need to just, “Get over it?”

V. CONCLUSION

The answer is of course, it depends. It is going to depend on several factors, the least of which will not be age. The Millennials and future generations will likely have much broader expectations of what is considered public, and therefore much narrower expectations of what is considered private. However, they will also likely value the right to privacy even more because while it is possible to imagine a future where less privacy exists, it is also possible to imagine a future where privacy will be regarded as even more precious and important to protect. Today’s youth seems to be embracing a more open, transparent, and inclusive way of life despite the traditional view that information is associated with power, and control of information is associated with controlling power. Thus, the real issue is going to be controlling the data.

Whether the government or private individuals and entities collect information, something needs to be done with data for it to have any usefulness and value. Otherwise, it is just “dark data” or data that is collected and stored, and for reasons such as the sheer volume, it is not cost effective or practical to do anything with the data. As technology continues to advance, that will change. We are already seeing evidence of this in the legal field. Advancement in data analytic technology, with things such as predictive coding, have already significantly altered strategies for the production and discovery of digital

evidence. Gone are the days of linear review and eyes on every document. There is just too much data for that approach.

As a general proposition, judges are on the forefront of this revolution recognizing that in the interest of judicial economy and professional responsibility, not only can technology be used, but it must be used. Several recent decisions have ordered the use of technology for discovery where it would be impractical and cost prohibitive to proceed without using technology.\(^{200}\)

The key is going to be finding qualified people to manage the data. People who are capable of making certain the data is being managed properly and responsibly.\(^{201}\) Used well, big data can be of value both to companies and consumers.\(^{202}\) There are many examples of data analytics being used to improve things, such as in healthcare, energy usage, safety, and efficiency.\(^{203}\) However, if data is not used responsibly, technology and big data could be dangerous.\(^{204}\)

The “Internet of Things” is one example of potential danger. The “Internet of Things” refers to the growing number of devices and items that are being embedded with some type of sensor or are otherwise connected to the Internet.\(^{205}\) With the nearly ubiquitous ability to be online nowadays through the spread of Wi-Fi networks, many devices are always connected to a network. This connection allows for the continuous collection of data, as well as in some cases, the ability to control the device.\(^{206}\) A device that might be considered to be a part of the “Internet of Things” is a Slingbox, which allows a person to control and watch his television while away from home via the Internet.\(^{207}\) Other examples include devices that provide people with the ability to control their home thermostats through applications on their smart phones.\(^{208}\) These conveniences are wonderful when they are working properly, but some analysts speculate that such technology could lead to actual physical threats in the future if someone finds a way to take over control of the devices, and could for example, raise the


\(^{201}\) See Counterterrorism and Privacy, supra note 205.

\(^{202}\) See id.


\(^{204}\) See Counterterrorism and Privacy, supra note 205.

\(^{205}\) See Gartner Says the Internet of Things Installed Base Will Grow to 26 Billion Units By 2020, GARTNER (Dec. 12, 2013), http://www.gartner.com/newsroom/id/2636073.

\(^{206}\) See id.


\(^{208}\) See Control and Monitor your Home from your iPhone, iPad or iPod touch, SMARTHOME, http://www.smarthome.com/iphone_apps.html (last visited Apr. 6, 2015).
temperature in a person’s home to the highest setting.209 Another example is the
future of automobiles. Vehicles are already starting to come with devices such as
GPS systems as standard equipment. These devices are monitoring your location
in order to provide you with route information; data about your location is being
collected and stored.210 Automobile manufacturers are currently working
together to develop stricter policies regarding the control and management of the
collected data, but they are still collecting it.211

Many are claiming that the next major development in automobile
technology will be cars that drive themselves.212 I know it seems farfetched, but
so did many of the things that we now take for granted a few years ago. I guess
we will have to wait and see and hope that even if the laws protecting privacy do
not keep pace with technological advancements, that the laws protecting people
from more immediate things will.

209. See Tom Brewster, There are real and present dangers around the Internet of Things,
GUARDIAN (Mar. 20, 2014, 9:00 AM), http://www.theguardian.com/technology/
211. See id.
212. See, e.g., Google Gets License to Operate Driverless Cars in Nevada, CNN (May 8, 2012,
REVERSE SUNSHINE IN THE DIGITAL WILD FRONTIER: PROTECTING INDIVIDUAL PRIVACY AGAINST PUBLIC RECORDS REQUESTS FOR GOVERNMENT DATABASES

Jennifer A. Brobst

ABSTRACT

In the present Digital Age, the American government engages in mass collection of information about individuals, and the databases with their layers of metadata that contain the information are then potentially subject to public disclosure pursuant to State and Federal Sunshine laws. In essence, what is occurring is a Reverse Sunshine effect, in which the lives of individuals, at times, are made more transparent than government action. North Carolina is the latest of a small number of states addressing the daunting question whether a single public records request may require production of a copy of an entire government database, potentially containing massive collections of individual information. While the North Carolina Supreme Court, like its sister states, managed to avoid directly answering the question, the specter of drastically increased commercial and individual access to government databases warrants caution. Until governmental agencies are better able to properly maintain and comply with public records requests for mass digital information, the risk of unwarranted disclosure of private information is great and the existing individual remedies and protections slight. Thus, it is timely to consider pragmatic and legislative solutions to more effective and tailored compliance with public records requests in the Digital Age, to empower individuals to enforce their right to privacy and to gain lawful access to public records.

---
* Jennifer A. Brobst, J.D., LL.M., is an Assistant Professor and Director of the Center for Health Law and Policy at Southern Illinois University School of Law. While the opinions herein are solely those of the author, special thanks are extended to William Polk, Special Counsel at the North Carolina Department of Public Safety, for his willingness to serve as a legal and policy sounding board for this work. Many thanks also to my new colleagues, Prof. Michele Mekel and Prof. Ryan Holte at Southern Illinois University School of Law, for their review and commentary on this work. Finally, I appreciate the assistance provided by the law review board students at Northern Kentucky Chase College of Law. Thank you for the opportunity to participate in the 4th Annual Law + Informatics Symposium on “Digital Evidence” sponsored by the Northern Kentucky Law Review and Northern Kentucky Chase College of Law on February 27, 2015.

“This is the age of total digitalisation; everything is online always.”
“Uh huh, and that’s why our politicians are pure and clean, and the world works so well, is it?
Because everybody knows everything and there’s no hiding place.”

Peter F. Hamilton, Great North Road (2012)

Overkill, overview
Over my dead body
Over me, over you
Over everybody


Davy Crockett: Well, me and Russel are figuring on heading down Texas way. That ain’t no place these days for a riverboat gambler with wobbly legs.

Thimblerig: There are times when cowardice is a virtue, my dear Colonel. It makes choosing a cause so very simple. Now, I know nothing about Texas of which you speak, but I do know of the fury of the outraged minions of the law. And as a consequence, I fear what lies behind me far more than the unknown that lies ahead.

KING OF THE WILD FRONTIER (Walt Disney Co. 1955).

I. INTRODUCTION

In the Digital Age of our early 21st century, the mill of government collection and public dissemination and re-collection and re-dissemination of information on citizens and government services consists of an unprecedented, churning mass of information. The resulting new balance between privacy and access to electronic government records as public information is precarious. Online government registries and databases expand the speed and size of information shared and collected, along with metadata which generates a depth

2. Information Age, WIKIPEDIA, http://en.wikipedia.org/wiki/Information_Age (last visited Mar. 22, 2015). (“The Information Age (also known as the Computer Age, Digital Age, or New Media Age) is a period in human history characterized by the shift from traditional industry that the industrial revolution brought through industrialization, to an economy based on information computerization. The onset of the Information Age is associated with the Digital Revolution, just as the Industrial Revolution marked the onset of the Industrial Age.”).

of detailed information previously unavailable to the public. State and Federal Sunshine Laws\(^4\) ensuring access to public records and open meetings, must be tempered by public policy concerns related to confidentiality, public safety, cost, and efficiency. Of course, the risk to privacy in the Digital Age is, of course, a longstanding concern.\(^5\) However, the development of “big data” capabilities, now combined with public records access, demands a closer examination of the sensitive balance of interests involved, specifically the interests of personal privacy, government resources, and government transparency.\(^6\)

Significantly greater public and private disclosure of information creates a new normal, arguably enhancing government accountability, but also reducing the individual’s power and autonomy to have a private life. Which interests prevail? The “Findings and Purposes” language of the Electronic Freedom of Information Act Amendments of 1996, signed by President Bill Clinton, envisioned the Digital Age as one of greater government accountability, but failed to mention any greater risk of intrusions on individual privacy.\(^7\) Envision the court clerk or public health official today, sitting behind a government desk,

---

4. See infra note 21.


managing public records requests for whole databases and layers of metadata within each database, operating within a digital frontier without adequate guidance, essentially without a sheriff easily at hand.\(^8\)

It is important to remember that a database is not merely a list of files, but an interactive tool “waiting to be asked a question,” where the query itself both creates and is part of a whole new record potentially different from the original inputted data.\(^9\)

Relational databases are not simple tables of cells like you see in an excel spreadsheet. Instead rows and fields are linked through foreign keys, primary keys, triggers and procedures across tables. Fields, rows, tables and even other databases may be related to each other through queries using Structured Query Language (SQL). The result is that, what often looks like a coherent set of data on an input form or a report may be scattered across multiple tables in a database, all subject to different levels of access based on rules enforced at either the application layer or data layer.\(^10\)

An obvious challenge of time, training and expense for the agency emerges, as well as an aggravated risk of over-compliance or under-compliance in response to the request. Many State agencies are encountering requests for the more nebulous term metadata in public records requests,\(^11\) but North Carolina is one of the few and most recent states to address whether an electronic copy of an entire government database may be requested as a single public record.\(^12\) Although not specifically addressed by the North Carolina courts, if one also requested the metadata within the whole database, the data points of information required to be produced as a public record would be legion.

In this new environment of public demand and well-funded commercial reach for digital public information, a lack of adequate control of the legal language and definition of electronic records in Sunshine laws will inevitably shift the balance of power to those with the greater and swifter voice.\(^13\) For those

---

8. If management of public records requests are eventually fully automated, then both the clerk and the sheriff would be out of town, machines left to mechanically and dispassionately sort and share the record of humanity.


10. Id.

11. See Blake A. Klinkner, *Metadata Redux: Now You’re Telling Me I Need to Provide Metadata to the Opposing Side?*, 37 Wyo. Lawyer 44, 45 (2014) (contrasting the national trend toward judicial discouragement of metadata access in discovery for lack of evidentiary value, with increasing legislative recognition of the importance of public records access to metadata).

12. See LexisNexis.

13. In addition to private and governmental interests, commercial interests in public records access to large data sets is another important facet to this discussion, as is commercial collection of private citizen data. See generally Stan Karas, *Privacy, Identity, Databases*, 52 Am. U. I. L. Rev. 393 (2002) (addressing corporate data mining and privacy rights). Neither will be discussed here in depth, nor will the actions and access of commercial technology companies contracted by the
aware of the absence of the sheriff in town, walking in and requesting information on everyone who ever had a run in with the law, or for a list of persons being treated for the latest health scare, is currently within sight. In fact, walking in now may now mean staying home and typing a few keys on a device to obtain instant access.

Whether government accountability has improved is unclear, but the public should recognize that the cacophony of public information is, at times, unmanageable and insecure, misleading and inaccurate, and appears to have already reduced the freedom, privacy, and autonomy of its individual citizens.\textsuperscript{14} To enhance government transparency and accountability, the defining purpose of Sunshine Laws, State and Federal Public Information Acts should use improved technology to highlight the activities of government officials. Instead, in the current Digital Wild Frontier, mass collection of information and database storage have tended to obfuscate government activity, instead shining a brighter, and at times glaring, light into the private worlds of its citizens: Reverse Sunshine in the Digital Wild Frontier.

Specifically, this article will focus first, in Section II below, on explaining the legislative policy of ensuring a balance of public and private interests in public records access.\textsuperscript{15} Part III addresses the quandary of Reverse Sunshine policies, in which the government’s mass collection of personal information converts public records access to access on individual lives rather than governmental functions.\textsuperscript{16} \textit{LexisNexis Risk Data Management Inc. v. North Carolina Administrative Office of the Courts}, recently decided by the North Carolina Supreme Court, will be reviewed as the last State decision to consider affirmatively permitting a single public records request for an electronic copy of an entire government database of information on individuals.\textsuperscript{17} Trends in the expansion of the use of government databases will be identified in Part IV, connecting the initial criminal justice databases to more recent public health surveillance databases and other non-criminal government monitoring of
government to maintain its complex databases be focused on at great length. The focus here is on the tensions emerging from governmental collection and placement of private citizen information in large databases, accessible to all through public records requests.

\begin{footnotesize} 
\begin{enumerate}
\item \textit{See infra Part II.}
\item \textit{See infra Part III.}
\item \textit{See infra Part III (discussing the recent LexisNexis decision).}
\end{enumerate}
\end{footnotesize}
individuals.\textsuperscript{18} In Part V, the lack of robust civil remedies to address unwarranted disclosure of private information in public records will be discussed in the context of increasingly difficult and complex compliance procedures by government clerks managing voluminous electronic collections of information.\textsuperscript{19} Finally, Part VI will assert the need for pragmatic and legislative solutions to ensure effective and proper stewardship of public access to government databases, with a view toward anticipated technological changes in the Digital Age.\textsuperscript{20}

II. A Balance of Interests in Public Records Access

Sunshine laws have defined the basic scope of public records and open meetings requirements for public bodies and agencies since the Cold War with limited effectiveness.\textsuperscript{21} The national trend is depicted as one of recent but enhanced government openness, at least initially: “[t]he increasing number of open legislative proceedings, coupled with statutes such as the Freedom of Information Act, 5 U.S.C. § 552, the Federal Advisory Committee Act, 5 U.S.C. §§ 1-14, and the Government in the Sunshine Act, 5 U.S.C. § 552b, establish at least this much.”\textsuperscript{22}

A. Government Transparency and Public Privacy in a Digital Age

Public records requests are therefore focused on the public’s “right to see” its government.\textsuperscript{23} State courts have consistently held that their respective Public Records Act “should be liberally construed and its exemptions should be

\begin{itemize}
\item \textsuperscript{18} See infra Part V.
\item \textsuperscript{19} See infra Part IV.
\item \textsuperscript{20} See infra Part VI.
\item \textsuperscript{22} B.H. v. McDonald, 49 F.3d 294, 303 (7th Cir. 1995) (noting that public records retention statutes have also supplemented core public records act statutes); see, e.g., Richard J. Pelz, Arkansas’s Public Records Retention Program: Finding the FOIA’s Absent Partner, 28 U. ARK. LITTLE ROCK L. REV. 175, 249 (2006) (“Arkansas is now on its way to the creation of a long-overdue records retention system that will serve as an essential counterpart to freedom of information and historical preservation.”).
\item \textsuperscript{23} Johnson v. Broussard, 118 So.3d 1249, 1255 (La. Ct. App. 2013) (“Whenever there is doubt as to whether the public has a right of access to certain records, the doubt must be resolved in favor of the public’s right to see.”).
\end{itemize}
narrowly construed in favor of disclosure.”

In his first day in office, President Barack Obama issued a Memorandum for the Heads of Executive Departments and Agencies on the Freedom of Information Act (FOIA), proclaiming, “All agencies should adopt a presumption in favor of disclosure, in order to renew their commitment to the principles embodied in FOIA, and to usher in a new era of open Government.”

Nevertheless, the call for openness in government accompanied a demand for openness from its citizens, such as applications of the Federal Intelligence Surveillance Act bulk telephony collection, without alerting or granting the citizenry an effective voice on this activity. Globally, the pendulum has swung back towards government secrecy despite a public outcry which has been understated and largely ineffectual.

That the stated policy of Sunshine laws is to “provide[] for liberal access to public records” is a double-edged sword when

---

27. For example, on January 1, 2014, Denmark enacted an exception to its freedom of information act, excluding public access to correspondence between government officials and civil servants when seeking advice, as well as ministers’ calendars. The largest citizen petition ever produced in Denmark (85,631 signatures) protested the change, and close to 1,500 protesters with torches appeared before the legislative building the night before enactment. However, thus far the amendment remains in effect. Peter Stanners, Freedom of Information Law Passes; Opponents Pledge Recall Vote, Copenhagen Post (June 4, 2013, 4:50 PM), http://cphpost.dk/news/freedom-of-information-law-passes-opponents-pledge-recall-vote.5486.html. In the United States, post-9/11 increased government secrecy has been purportedly justified based on national security and the imminency of terrorist threats. However, a U.S. Senate report release of CIA documents from 2001-2006 disclosed repeated misrepresentation by the CIA to the government and media of the extent of torture and harsh interrogation techniques; and the White House administration has legally fought against more related disclosures in response to a New York Times Freedom of Information Act request. Bruce Zagaris, U.S. Senate Releases Report on U.S. Government Torture During the War on Terrorism, 30 No. 15 Intern’l Enforcement L. Rep. 560 (2014) (discussing New York Times Co. v. U.S. Dept. of Justice). The final finding of the Senate report states: “20. The CIA’s Detention and Interrogation Program damaged the United States’ standing in the world, and resulted in other significant monetary and non-monetary costs.” Id. Arguably, one non-monetary cost goes to the heart of the theory of Sunshine Laws, i.e., ensuring public trust and government accountability. An amicus brief filed in The New York Times Co. v. U.S. Dept. of Justice states in its introduction: “As the Executive Branch continues to classify millions of documents—more than at any time in our nation’s history-- it simultaneously asks the judiciary to rubber stamp its classification decisions.” Brief for Reporters Committee for Freedom of the Press, et al. as Amici Curiae Supporting Appellees at 1, New York Times Co. v. U.S. Dept. of Justice, 752 F.3d 123 (2d Cir. 2014) (Nos. 13-422, 13-445), 2013 WL 1791132.
public records primarily contain information on private individuals rather than information on government officials.

The United States Supreme Court in *U.S. Department of State v. Ray*, succinctly identified the primary emphasis on disclosure underlying Sunshine Laws, particularly in the context of withholding from public access records that may involve medical, personnel, and other confidential records:

> The Freedom of Information Act was enacted to facilitate public access to Government documents. *John Doe Agency v. John Doe Corp.*, 493 U.S. 146, 151, 110 S.Ct. 471, 475, 107 L.Ed.2d 462 (1989). The statute was designed “to pierce the veil of administrative secrecy and to open agency action to the light of public scrutiny.” *Department of Air Force v. Rose*, 425 U.S. 352, 361, 96 S.Ct. 1592, 1599, 48 L.Ed.2d 11 (1976). Consistently with this purpose, as well as the plain language of the Act, the strong presumption in favor of disclosure places the burden on the agency to justify the withholding of any requested documents. *Ibid.; Department of Justice v. Reporters Comm.*, 489 U.S., at 755, 109 S.Ct., at 1472. That burden remains with the agency when it seeks to justify the redaction of identifying information in a particular document as well as when it seeks to withhold an entire document. See 5 U.S.C. § 552(a)(4)(B).

In response to criticism of unwarranted intrusion by the government into private lives, Congress has made some effort to protect individual privacy rights in amending the Electronic Communications Privacy Act. One amendment would limit government access to private electronic communications, including limitations on whether the government could access a person’s text message content from a third party carrier. Note that most of the recent proposed amendments to further strengthen personal online privacy have not passed or have been given a negligible chance of being enacted. Withholding from the public access to government information that may compromise national security and public safety is unquestionably important. However, the simultaneous trend in the Digital Age towards increasing government privacy while reducing individual privacy is a matter of significant concern. Fortunately, many States...
do not assert that the Federal Freedom of Information Act governs interpretation of State public records laws.\textsuperscript{34} This has allowed States to work toward enhancing transparency and tailoring their provisions to State and regional needs, separate and apart from the purported Federal interest in national security.\textsuperscript{35}

When assessing government choices in collecting mass information, or what personal information may be of value as a matter of public record, many would accept that certain personally identifiable information is worthy of open access for society to function, such as records of births and deaths. Legal matters may by nature justify public record status, such as marriage and divorce records or home ownership and property records, so that the legal system can function properly and protect respective legal rights and responsibilities. Yet some personal or legal matters that would benefit the public if disclosed, also bear particular social stigmas or invasions of protected privacy such as immigration status, debt and bankruptcy status, criminal history or health risk status. What occurs in a person’s life between those moments of birth and death is more personal and more sensitive, the expression of what constitutes the choices and experiences of the individual.\textsuperscript{36} This need for care in a Digital Age, determining what personal information is collected and how it is disclosed, warrants scrutiny of any reckless or ill-defined governmental approach to the creation and maintenance of government databases.


\textsuperscript{35} See generally Monique C.M. Leahy, \textit{Proof Supporting Disclosure Under State Freedom of Information Acts}, AM. JUR. PROOF OF FACTS 3d 1 (2013) (noting in section 1 the variation among states from the Federal FOIA provisions, and including in section 6 a state by state listing of freedom of information acts); Christopher P. Beall, Note, \textit{The Exaltation of Privacy Doctrines Over Public Information Law}, 45 DUKE L.J. 1249, 1285 (1996) (“This [Federal] tendency to value privacy over access is all the more noteworthy because some States have shown a contrary trend in recent amendments to their public records laws.”).

\textsuperscript{36} As Henry Altman, played by actor Robin Williams, opined in his hospital bed, “On my tombstone it will say, Henry Altman, 1951 dash 2014. I never knew ‘til now, it’s not the dates that matter. It’s the dash.” \textit{THE ANGRIEST MAN IN BROOKLYN} (Lionsgate 2014).
B. Broad Public Records Definitions Encompass Technological Change

In the midst of our current social transformation, public and private leaders should closely monitor and understand the trends in expanding public records access to digital information. As discussed more fully below, criminal databases and registries tend to act as a precursor to expanded sharing of personal information in other government contexts.37 Even more private than criminal records, and much more numerous, are medical records. Although Sunshine laws have well known exceptions enacted to ensure the privacy of an individual’s medical information, under the State’s police power, public health policies and regulations may mandate or permit disclosure, especially with regard to medical information maintained by governmental agencies and state owned facilities.38

As an example of State application, pursuant to North Carolina General Statutes section 132-1(a), public records are generally defined as documentary material “made or received pursuant to law or ordinance in connection with the transaction of public business by any agency of North Carolina government or its subdivision.”39 Note that aside from the content of medical records, the form of such records would fit the statutory definition.40

N.C.G.S. § 132-1. “Public records” defined

(a) “Public record” or “public records” shall mean all documents, papers, letters, maps, books, photographs, films, sound recordings, magnetic or other tapes, electronic data-processing records, artifacts, or other documentary material, regardless of physical form or characteristics, made or received pursuant to law or ordinance in connection with the transaction of public business by any agency of

37. See infra Part IV.A.
38. See infra Part IV.B. See, e.g., Child Prot. Grp. v. Cline, 351 S.E.2d 541, 543 (W.Va. 1979) (upholding the public’s need to know against the medical privacy interests of a reinstated public school bus driver with apparent mental health problems). The West Virginia Supreme Court of Appeals interpreted the freedom of information exception in W. Va. Code § 29B-1-4(2) (1980), which states: “Information of a personal nature such as that kept in a personal, medical or similar file, if the public disclosure thereof would constitute an unreasonable invasion of privacy, unless the public interest by clear and convincing evidence requires disclosure in the particular instance . . .” Note also that the patent system has been described by some as the first Sunshine law, requiring public disclosure of inventions, which have for several decades included microorganisms developed in medical research. See Bradford C. Auerbach, Biotechnology Patent Law Developments in Great Britain and the United States: Analysis of a Hypothetical Patent Claim for a Synthesized Virus, 6 BOSTON COLLEGE INT’L & COMPAR. L. REV. 563, 582 (1983).
39. (emphasis added).
40. N.C. GEN. STAT. § 132-1 (emphasis added) (medical records for the purpose of this manuscript primarily include records that contain health information, but may occasionally include records on the qualifications and investigations of service providers, and the business functions of health institutions); see, e.g., Knight Pub. Co. v. Charlotte-Mecklenburg Hosp. Auth., 616 S.E.2d 602 (N.C. Ct. App. 2005) (addressing a newspaper publisher’s action against a public hospital under the Public Records Act and the Public Hospital Personnel Act, seeking disclosure of information regarding non-salary benefits and expense reimbursements paid to seventeen current or former employees of the hospital).
North Carolina government or its subdivisions. Agency of North Carolina government or its subdivisions shall mean and include every public office, public officer or official (State or local, elected or appointed), institution, board, commission, bureau, council, department, authority or other unit of government of the State or of any county, unit, special district or other political subdivision of government.

(b) The public records and public information compiled by the agencies of North Carolina government or its subdivisions are the property of the people. Therefore, it is the policy of this State that the people may obtain copies of their public records and public information free or at minimal cost unless otherwise specifically provided by law. As used herein, “minimal cost” shall mean the actual cost of reproducing the public record or public information.

As in most jurisdictions, the public records, as well as the public information obtained by North Carolina government agencies and its subdivisions, are the “property of the people” and therefore must be made available to the public for free or at low cost. Moreover, the burden is on the agency to assert that the information is exempt and not within the definition of a public record or that it fits within an exception. As seen in North Carolina, the recent judicial focus on public records access to databases and other new forms of compiling information have usually found public records accessibility governed by terms such as “electronic information” or a catch-all term such as “other documentary material.” At this time, no State or Federal statute has explicitly prohibited public access to records in the form of a database. That is, the broad definition of electronic information or the catch-all terms for form of record usually found in public records statutes allows for continued public records requests for entire databases, if the request clearly defines what form is sought.

As State and Federal governments zealously collect personal information in the interests of public safety or public health, information then fed back to the public as public information, the practice bears some risks. Must a person requesting a public record justify why the record is requested? The answer is generally no, because the purpose of Sunshine laws is government transparency rather than public use. A public alert can tell citizens to watch out for strangers and lock their doors at night without telling them in a Sex Offender Registry that a sex offender lives next door. A public alert can inform citizens to avoid people with fevers and coughs who have recently traveled to West Africa, without

42. See U.S. Dept. of State v. Ray, 502 U.S. 164, 173 (1991) (internal citations omitted) (“Consistently with this purpose, as well as the plain language of the [Federal Freedom of Information] Act, the strong presumption in favor of disclosure places the burden on the agency to justify the withholding of any requested documents.”).
43. See infra Part III.A (discussing LexisNexis).
telling them that a person who survived ebola lives next door.\textsuperscript{45} Not all information made available by the government will be prudent to share even if it appears justified in the public interest.

But it is also a question of distrust of the government’s stated purpose in collecting information, informed in part by constitutional rights of privacy at both State and Federal levels,\textsuperscript{46} if not yet a fully recognized constitutional due process right to informational privacy after \textit{NASA v. Nelson}.\textsuperscript{47} For example, the Florida Constitution provides: “Every natural person has the right to be let alone and free from governmental intrusion into the person’s private life except as otherwise provided herein. This section shall not be construed to limit the public’s right of access to public records and meetings as provided by law.”\textsuperscript{48} The official commentary to this State constitutional amendment suggests a legislative reliance on Justice Brandeis’s famous dissent in \textit{Olmstead v. U.S.},\textsuperscript{49} that is, that the Makers of the Constitution in seeking to protect the pursuit of happiness “conferred, as against the government, the right to be let alone – the most comprehensive of rights and the right most valued by civilized men.”\textsuperscript{50} Many broad legal definitions of the accepted form of public records access encompass the massive size of electronic government databases, with little heed to the right to be let alone.

\textbf{C. Mass Collection of Information on Private Individuals by the Government Today}

When authorized, the mass information collected by the government and organized in databases and registries is collected under the auspices of various public purposes. Some information is mandated for collection, while other

\textsuperscript{45} See, e.g., Guinea: Life After Ebola Has New Meaning for Two Survivors Now Helping Others, \textit{World Health Org.}, (July 2014), http://www.who.int/features/2014/life-after-ebola/en/ (providing a first person account from survivors of the Ebola virus who state that “[t]he stigma is so strong they prefer not to use their real names or show their faces in print”).


\textsuperscript{47} \textit{Cf. NASA v. Nelson}, 562 U.S. 134, 138 (2011) (Alito, J.) (“We assume, without deciding, that the Constitution protects a privacy right of the sort mentioned in \textit{Whalen} and \textit{Nixon}.”) with id. at 160 (Scalia, J., concurring) (“A federal constitutional right to ‘informational privacy’ does not exist.”). \textit{See also} Warner v. Township of South Harrison, 885 F.Supp.2d 725, 739 (D.N.J. 2012) (reading the holding in \textit{NASA} “as an affirmation that a person has a constitutional right to be free from undue disclosure of private information and that the balancing test articulated in \textit{Fraternal Order of Police . . .} is a proper way to balance the competing individual and governmental interests at stake.”).


\textsuperscript{50} \textit{Olmstead}, 277 U.S. at 479 (Brandeis, J., dissenting).
information is collected without legal mandate because it is in the public domain. In the Digital Age, legally defining what constitutes the “public domain” is an important matter of debate.

For example, the bulk telephony metadata collection by U.S. national intelligence agencies has been re-authorized multiple times. The collection of bulk telephony metadata from the public at large includes collection of to/from headers, dates and subject lines in emails, but not the content within messages. In 2014, the National Security Administration (NSA) discontinued this collection, and documents were requested by the Electronic Privacy Information Center subject to the Freedom of Information Act to shine a light on the actions of the NSA regarding this program. As much as the public disliked the government’s perceived intrusion into its private communications, it may equally object to other members of the public receiving this information through public records requests. The program for bulk collection from telephone companies was meant to build in sufficient checks and balances to protect the information, but by


Following a declassification review by the Executive Branch, the DNI has released in redacted form the March 28, 2014 Primary Order, signed by Judge Rosemary M. Collyer. Separately, following a declassification review by the Executive Branch, the FISC published in redacted form the June 19, 2014 Primary Order and an accompanying Memorandum Opinion, signed by Judge James B. Zagel, re-authorizing the collection of bulk telephony metadata under Section 215. The most recent authorization expires on September 12, 2014. These Primary Orders and Memorandum Opinion re-affirm that the bulk telephony metadata collection is lawful.


2009 it came to light that the NSA had internal compliance problems with the checks system.\textsuperscript{54}

That particular NSA program may have ended, with assurances that the bulk information collected was purged, but a temporary new program took its place similar in purpose but requiring greater judicial oversight, with individual requests rather than bulk collection.\textsuperscript{55} In the meantime, with the USA Freedom Act Congress is considering a new bill to define the parameters of Federal Bureau of Investigation (FBI) requests for information related to international terrorism or espionage.\textsuperscript{56} The bill also potentially “bars information concerning any U.S. person acquired from such production from being used or disclosed in any other manner by Federal officers or employees without the consent of such person, except with approval of the Attorney General if the information indicates a threat of death or serious bodily harm.”\textsuperscript{57} Clearly, the Federal government intends to continue to collect massive amounts of information on Americans. In a Digital Wild Frontier, the enhanced ability and government interest in creating big data and Reverse Sunshine, that is, public records access to personal information, without adequate individual privacy protections, inevitably compromises individual rights.

Admittedly, exemptions and confidentiality laws are in place to accommodate privacy interests in Public Records Acts.\textsuperscript{58} Also, to serve the public interest, including the ability of government to carry out its essential and self-sustaining functions, the law permits (and at times mandates) collection of large-scale information on its citizens. When this occurs, government must

\textsuperscript{54} \textit{Id.} The checks and balances required that the information could be used only for counterterrorism purposes. Furthermore, this information had to be stored in secure databases. In addition, the databases could be queried using an identifier such as an email address only when an analyst had a reasonable and articulable suspicion that the email address was associated with certain specified foreign terrorist organizations that were the subject of FBI counterterrorism investigations. The basis for that suspicion had to be documented in writing and approved by a limited number of designated approving officials identified in the Court’s Order. Moreover, if an identifier was reasonably believed to be used by an individual in the United States, NSA’s Office of General Counsel would also review the determination to ensure that the suspected association was not based solely on First Amendment-protected activities; and finally, the NSA was required to destroy the bulk metadata after a set period of time.

\textsuperscript{55} Joint Statement from the Office of the Director of National Intelligence and the Department of Justice on the Declassification of Renewal of Collection Under Section 501 of the Foreign Intelligence Surveillance Act, DOJ 14-655, 2014 WL 2795448 (June 20, 2014).

\textsuperscript{56} USA Freedom Act, H.R. 3361, 113th Cong. (2014) (passed the House on 5/22/2014 and referred to the Senate, but remaining in the Select Committee on Intelligence without further action) (https://beta.congress.gov/bill/113th-congress/house-bill/3361). Note that other bills were introduced in the 2013-2014 Congressional Session, which also opposed bulk telephone metadata collection by the intelligence services under the Foreign Intelligence Surveillance Act of 1978, including the Civil Liberties Protection Act (S. 2093, 113th Cong. (2014)), Telephone Surveillance Accountability Act (H.R. 2684, 113th Cong. (2014)), and Telephone Metadata Reform Act (H.R. 3875, 113th Cong. (2014)).

\textsuperscript{57} \textit{Id.} (summary).

\textsuperscript{58} \textit{See infra} section IV(B)(1).
effectively maintain the information and determine the need for exemptions from public records definition and exceptions from public records access. For example, multiple State Child Abuse Registries, identifying parents under investigation, have resulted from the mandatory reporting statutes and policies.\(^{59}\) However, statutory exemptions preclude public access to this information, which is to be held “in the strictest confidence,” at least at the present time.\(^{60}\)

Any examination of public records involving government databases must question the justification for the collection of the information in the first place and how it is maintained. In addition to the more recent issues addressed above with NSA bulk telephony collection,\(^{61}\) Federal collection of personal information on American citizens using data mining and sweeping surveillance is well known to have begun by the Department of Defense after 9/11, eventually shifting to the purview of the NSA.\(^{62}\) From the beginning, critics held it to be unjustifiably intrusive and ineffective: “If you have an idea of what you are looking for, you do not need data mining. If you do not, data mining will only provide excuses for indulging your prejudices.”\(^{63}\)

In contrast to mandatory collection, when individuals voluntarily provide information in the public domain, such as uploading images of child pornography, then even the metadata containing GPS coordinates within the images have been deemed legitimately accessible to government data mining: “Whether an individual lacks a privacy interest in dialed numbers because those numbers are necessarily disclosed to his phone company is a much different question than whether an individual loses his privacy interest in an item because he voluntarily makes it publicly available on the internet.”\(^{64}\) Note that in North

\(^{59}\) See Child Welfare Information Gateway, Establishment and Maintenance of Central Registries for Child Abuse Reports (2014), https://www.childwelfare.gov/topics/systemwide/laws-policies/statutes/centreg/ (last visited Feb. 12, 2015) ("Central registry reports are typically used to aid social services agencies in the investigation, treatment, and prevention of child abuse cases and to maintain statistical information for staffing and funding purposes.").


\(^{62}\) See generally, Doug Mataconis, Would N.S.A. Data Mining Have Been Able to Stop 9/11?, Outside Beltway (Dec. 30, 2013), http://www.outsideebeltway.com/would-n-s-a-data-mining-have-been-able-to-stop-911/ (arguing that the ineffectiveness of the N.S.A. data mining efforts to reduce terrorist attacks justify judicial limitations on warrantless searches of domestic activities).


Carolina, the State government’s 911 database is now subject to privacy protections for the individuals who call.\textsuperscript{65}

N.C. Gen. Stat. § 132-1.5. 911 database

Automatic number identification and automatic location identification information that consists of the name, address, and telephone numbers of telephone subscribers, or the e-mail addresses of subscribers to an electronic emergency notification or reverse 911 system, that is contained in a county or municipal 911 database, or in a county or municipal telephonic or electronic emergency notification or reverse 911 system, is confidential and is not a public record as defined by Chapter 132 of the General Statutes if that information is required to be confidential by the agreement with the telephone company by which the information was obtained. Dissemination of the information contained in the 911, electronic emergency notification or reverse 911 system, or automatic number and automatic location database is prohibited except on a call-by-call basis only for the purpose of handling emergency calls or for training, and any permanent record of the information shall be secured by the public safety answering points and disposed of in a manner which will retain that security except as otherwise required by applicable law.

Perhaps it is less concerning when personal information is provided to the government voluntarily. Examples of voluntary provision of information to the government, and resulting storage in databases of public record, include those comprised of Board of Elections voter information,\textsuperscript{66} records of licensing boards related to professional licensure,\textsuperscript{67} and State employee salaries.\textsuperscript{68}

In the future, as companies increase the use of biometric scanning of fingerprints and retinal scans as an effective means of security, the government

\textsuperscript{65} N.C. GEN. STAT. § 132-1.5 (emphasis added).

\textsuperscript{66} Voter registration information is generally collected in one of the most prominent and easily searched databases available online. See, e.g., N.C. PUBLIC VOTER SEARCH, https://www.ncsbe.gov/webapps/voter_search/ (last visited Apr. 10, 2015). By a simple name search, a person’s full name, home address, race, ethnicity, gender, party affiliation, DMV driver’s registration, and dates of past voting are made available by the government for all to see online. Id.


may be able to access and collate this information as well. Of course, law enforcement already collects this information for licensure and arrestee information. For example, the North Carolina licensed childcare providers must submit to fingerprinting background checks, which are then compared with State Bureau of Investigation and FBI fingerprint databases. Whether this form of identifying information is deemed confidential, particularly when it involves fingerprint and other physical remnants of our presence left everywhere in public, determines whether these databases should be accessed by individuals and commercial entities as public records.

II. THE REVERSE SUNSHINE DILEMMA: PUBLIC RECORDS LAW APPLIED TO GOVERNMENT DATABASES AFTER LEXISNEXIS

When the government engages in data mining and mandated or voluntary collection of personal information, the use of databases and registries facilitates the government’s ability to search and interpret the data on a large scale. The legal authority determining whether this information is then made available to the public as a matter of public record are discussed below, specifically with respect to requests for entire databases along with the metadata within them. As technology improves and becomes more cost efficient, a nascent trend in expanding access to entire databases as public records is emerging. However, some existing restrictions on voluminous records requests, as well as new restrictions on public access to proprietary government software code have been enacted, both concerned more with protecting government functions than the privacy of the records of individuals contained within these massive databases.

A. Expanding Public Access to Public Records

Recall that databases and registries as compilations of public information are often impliedly included in the definition of an accessible form of public record. Whether this includes the metadata within the database, or the database in a particular form, has been dependent largely on judicial interpretation in the absence of statutory specificity. The most recent state interpretation of the definition of a public record with respect to a request for an entire database is


71. See N.C. DIVISION OF CHILD DEVELOPMENT, Live Scan Fingerprinting Option for Child Care Providers, http://ncchildcare.dhhs.state.nc.us/pdf_forms/Live_Scan_Fingerprint_Option.pdf (last visited July 8, 2015).

72. See infra Section III(B).
LexisNexis Risk Data Management Inc. v. North Carolina Administrative Office of Courts,\textsuperscript{73} recently decided by the North Carolina Supreme Court.

1. Public Records Requests for an Entire Government Database

While public records requests for databases as a whole are of relatively recent origin, until recently, the few State courts that had addressed the question (ten to fifteen years ago) had for varying reasons held that the government could withhold access.\textsuperscript{74} However, within the last five years, some State courts accustomed to the expansion of government database use began to grant public records access to a copy of the facial information in the databases, without accompanying metadata.\textsuperscript{75} In 2014, the North Carolina Court of Appeals in LexisNexis not only held that such a request could be granted, but that as an electronic copy was requested, it should be provided in that form.\textsuperscript{76} As will be discussed below, the North Carolina Supreme Court reversed and remanded on the basis that a more recently enacted, narrow statute governed public access to government criminal records databases, rather than the Public Records Act which the Court of Appeals had relied on.\textsuperscript{77}

Two segments of the LexisNexis corporate group, one from Florida and another from Georgia, sought access to the non-confidential information in the North Carolina Automated Criminal/Infraction System database (ACIS), for the purpose of including that information in national digital access public records services for paying customers.\textsuperscript{78} The North Carolina county clerks denied the request because they only maintained their own county records in ACIS. In turn, the North Carolina Administrative Office of the Courts (AOC) staff denied the request because they did not create the county records, but simply created and maintained ACIS as a “mainframe application which serves as a record-keeping tool for clerk of court statewide.”\textsuperscript{79}

Initially, the Wake County Superior Court in LexisNexis held that ACIS is not a public record separate and distinct from the individual public criminal records within it, particularly when remote access to ACIS records is already

\textsuperscript{73} LexisNexis, supra note 1.

\textsuperscript{74} See, e.g., LexisNexis. But see Coronado Police Officers Ass’n v. Carroll, 131 Cal. Rptr. 2d 553 (Cal. Ct. App. 2003) (denying a public records request for a database of offenders maintained by a county public defender’s office); Crutchfield v. New Mexico Dept. of Taxation & Revenue, 106 P.3d 1273 (N.M. Ct. App. 2004) (denying a request seeking to obtain an electronic copy of the entire severance tax database as well as continuous monthly updates).

\textsuperscript{75} See Maese v. Davis, Cnty, 273 P.3d 949, 951 (Utah Ct. App. 2012) (holding that a request for a “copy of the database or a twenty-year transaction report” of property records was not a request for the “database itself” and its accompanying metadata and “other variables”).


\textsuperscript{77} LexisNexis at *6.

\textsuperscript{78} LexisNexis (Ct App), 754 S.E.2d at 225.

\textsuperscript{79} Id. at 225-26.
made available to the public. Judge Hardin concluded in his order that “Defendant AOC is not the custodian of the criminal records stored in the ACIS database and did not, therefore, violate the Public Records Act in responding to the plaintiffs that it had no records responsive to their request for a copy of the entire ACIS database.”

The court was also concerned that releasing a copy of the database in its entirety would permit the Defendant, a commercial entity, to “enter into one or more nonexclusive contracts with third parties to provide remote public access to records stored in ACIS.” The Superior Court therefore dismissed the LexisNexis Plaintiffs’ motion for judgment on the pleadings, and granted the Defendants’ (State agents and agency) responsive motion.

However, the North Carolina Court of Appeals disagreed and reversed the trial court order as to the AOC. Applying North Carolina General Statute section 132-1(a), the North Carolina Court of Appeals looked to the specific terms “electronic data-processing records” and “other documentary material, regardless of physical form or characteristic” in holding that an electronic government database is itself a public record.

The court also defined a database as a public record using its dictionary definition:

> [a] collection of data or information organized for rapid search and retrieval, especially by a computer. Databases are structured to facilitate storage, retrieval, modification, and deletion of data in conjunction with various data-processing operations. A database consists of a file or set of files that can be broken down into records, each of which consists of one or more fields. Fields are the basic units of data storage. Users retrieve database information primarily through queries. Using keywords and sorting commands, users can rapidly search, rearrange, group, and select the field in many records to retrieve or create reports on particular aggregates of data according to the rules of the database management system being used.

---


82. Id. at 4.
83. Id.
84. LexisNexis (Ct App), 754 S.E.2d at 226.
As a result, the North Carolina Court of Appeals in *LexisNexis* would allow a private corporation to make a public records request for an electronic copy of the entire ACIS database at minimal cost. Apart from the core Sunshine argument for transparency, other policy arguments can be made for a public benefit permitting this event. Although the North Carolina Court of Appeals never expressly explained how a database is different from the records within it, public access to digital public records improves with innovative compilations across the various government databases, as well as reorganization of the records within them. In the amicus brief filed by the Consumer Data Industry Association in *LexisNexis*, representing private companies collating and disseminating public information for a fee to consumers and government agencies, the financial impact to their interests is made clear if the Supreme Court determines that a whole database is not a public record: “access to databases across the state government would be subject to restricted access, adversely affecting investigations, slowing commercial transactions and mortgages, and impacting other transactions that rely on public record information.”

Ultimately, the North Carolina Supreme Court did not agree with the lower court’s interpretation of the issues, avoiding a significant impact on the State’s contracts with vendors to create similar government databases in North Carolina. The Court of Appeals had acknowledged the following risk:

> We are sympathetic to the AOC’s argument that, if copies of the entire ACIS database are available upon request under the Act, third parties may be discouraged from entering into “contracts under reasonable cost recovery terms . . . to provide remote electronic access to [court] records. . . . “ . . . If provision of copies of ACIS under the Act renders the option of providing remote electronic access unnecessary or not cost-effective, the AOC can simply decline to offer this additional method of access.

The Court of Appeals implied that the resolution to this financial dilemma for the government would be to no longer offer the public remote access to an online database of criminal record information; or the government could advocate for legislative reform by adding a “clear statutory exemption or exception” for entire databases within the definition of a public record. Otherwise, public records “must be made available for public inspection.”

87. *LexisNexis* at *6 (noting that commercial entities do not have unfettered public records access to criminal databases, but may contract with the government for specialized access pursuant to N.C. Gen. Stat. § 109(d)).
88. *LexisNexis (Ct App)*, 754 S.E.2d at 229 (internal citation omitted) (emphasis added).
89. *Id.* (relying on *News & Observer Pub. Co. v. Poole*, 412 S.E.2d 7, 19 (N.C. 1992)).
90. *Id.*
The North Carolina Supreme Court instead interpreted the state statutory scheme as providing a narrow statute limiting the forms of access to electronic records, including criminal databases, under North Carolina General Statutes chapter 7A, section 109(d).\(^91\) The court reasoned that section 109(d) is “a more specific statute that overrides applicability of the Public Records Act here,” such that remote electronic access to entire systems would be available through nonexclusive licensing contracts only.\(^92\) Section 109 addresses public access as follows:

(a) Each clerk shall maintain such records, files, dockets and indexes as are prescribed by rules of the Director of the Administrative Office of the Courts. Except as prohibited by law, these records shall be open to the inspection of the public during regular office hours, and shall include civil actions, special proceedings, estates, criminal actions, juvenile actions, minutes of the court, judgments, liens, lis pendens, and all other records required by law to be maintained. . . .

(d) In order to facilitate public access to court records, except where public access is prohibited by law, the Director may enter into one or more nonexclusive contracts under reasonable cost recovery terms with third parties to provide remote electronic access to the records by the public. Costs recovered pursuant to this subsection shall be remitted to the State Treasurer to be held in the Court Information Technology Fund established in G.S. 7A-343.2.\(^93\)

Notably, the Supreme Court did not address the Court of Appeals’ determination that the database itself was a newly created single record.\(^94\)

This absence of clarification could potentially create confusion for the public interested in making public records requests for entire databases not subject to section 109(d), which is specifically directed toward court records. In fact, even the North Carolina Court of Appeals in *LexisNexis* never clearly defined what an “electronic copy” meant, although it held that an entire database would qualify.\(^95\) The North Carolina Supreme Court leaves to the legislature the onus of better defining a database as a single electronic record under the Public Records Act and related statutes. Indeed, a new statutory provision addressing proprietary database software was recently enacted,\(^96\) but no other legislative clarification or restriction on access has been made in North Carolina to date. However, as

---

91. *LexisNexis* at *1.
92. *Id.*
94. *See LexisNexis* at *5* (“Because this statute [section 109(d)] does not refer to the “custodian” of the pertinent records, we need not address arguments that are dependent on a determination of who is the custodian of ACIS and the records included in that database”).
95. *LexisNexis (Ct. App)*, 754 S.E.2d at 229 (stating only that “Lexis is not seeking remote electronic access to ACIS, but rather has requested a copy of the entire database”).
96. *See infra* Section III(B)(1).
discussed below, at least one other State legislature, Utah, has effectively narrowed access to public records database formats.97

*LexisNexis* and other State court opinions relating to public records requests for whole databases consistently rely on the language and scope of the public records statute. In New Mexico, a commercial entity seeking a state tax severance database as a matter of public record, as well as monthly updates, was not permitted free access because the state public records law had foreseen this type of request and would have required either royalties or a licensing agreement, which the government and corporation were unwilling to agree upon.98 In short, in New Mexico, significant costs might restrict commercial public records requests of this nature, but the legislature did not prohibit release of an entire database of information as a matter of public record.

In a split decision, the California Court of Appeals upheld denial of access by a law enforcement association to a county public defender’s database of offender information. As in New Mexico, the court interpreted the public records statute to possibly permit access to an entire database, but it found that there was a privacy exemption to the information itself.99 The majority held that this particular database did not exist to perform a government function, but was instead a service to individual indigent clients as was therefore exempt from disclosure. As stated in the majority opinion: “We do not accept the dissent’s position that the database is a public record merely because the storage medium makes information in client files easily accessible or because some of the information in the database (though obtained from public sources) did not originate from a particular client file or is shared by more than one client.”100 In turn, the dissent focuses in part on the nature of a database itself, inferring that its creation by the government is itself a government function accessible to the


98. Crutchfield v. New Mexico Dept. of Taxation and Revenue, 106 P.3d 1273, 1276 (N.M. Ct. App. 2004). The applicable statute, N.M. Stat. § 14-3-15.1(C), provided:

C. The state agency that has inserted data in a database may authorize a copy to be made of a computer tape or other medium containing a computerized database of a public record for any person if the person agrees:

1. not to make unauthorized copies of the database;
2. not to use the database for any political or commercial purpose unless the purpose and use is approved in writing by the state agency that created the database;
3. not to use the database for solicitation or advertisement when the database contains the name, address or telephone number of any person unless such use is otherwise specifically authorized by law;
4. not to allow access to the database by any other person unless the use is approved in writing by the state agency that created the database; and
5. to pay a royalty or other consideration to the state as may be agreed upon by the state agency that created the database.


100. *Id.*
people: “How can it be that records owned and compiled by a government agency, stored and maintained with public funds, that include both public and private information about individual citizens, regardless of their profession, are other than public records?”101

For various reasons, these decisions managed to avoid the issue of whether a database is defined as a single public record, which ultimately occurred in North Carolina as well after the Supreme Court ruled on other grounds in _LexisNexis_. Louisiana’s Court of Appeals most closely reaches the same conclusion as the North Carolina Court of Appeals in _Johnson v. Broussard_,102 in which a pharmacy association requested a digital copy of a computer database managed by the Louisiana Board of Pharmacy. Although the Louisiana Court of Appeals in _Johnson_ held that the extensive database information requested was within the purview of the electronic records access permitted by the Public Records act, the request was never made for the entire database, but only for segments of it.103 In _Maese v. Davis Cnty_, the Utah Court of Appeals clearly stated that it did not need to reach the question of whether a whole database could be the subject of a single public records request, because the requestor gave an alternative to the acceptable forms of information supplied and the State satisfied its obligations by allowing on site access to the public face of the database.104

In a Digital Age, where the volume and complexity of personal information maintained by the government is easily stored and disseminated, the courts are clearly beginning to send a sharp message to legislatures. The message in _LexisNexis_ and its earlier sister cases reminds the legislature that it must either amend Sunshine Laws to limit access, or the courts will force disclosure of mass information in databases as a matter of public record to abide by the underlying policy promoting government transparency. Unfortunately, the privacy interests of individuals whose information is the subject of these requests appears to be a secondary concern for both branches of government.

2. Public Records Requests for Metadata

As the judiciary grapples with defining the proper scope of public records requests for databases, it appears that no state has adopted a strict limitation on public records requests for metadata, although an emerging body of case law has interpreted the appropriate scope of such a request.105 The definition of what

101. _Id._ at 565.
103. _Id._ at 1251.
105. See, e.g., _Nervik v. State Dep’t of Licensing_, No. 41834-7-II, 2012 WL 5503431, at *1 (Wash. Ct. App. Nov. 13, 2012) (holding that a public records request for email does not automatically include associated metadata without a more specific request); _O’Neill v. City of Shoreline_, 240 P.3d 1149 (Wash. 2010) (finding as a matter of first impression that certain hidden metadata “pertaining to” a single email is subject to disclosure under the state Public Records Act);
constitutes metadata is by no means settled, and “data about data” is as clear as mud. In the production of official governmental electronic records, metadata may be built in deliberately as a component meant to be accessed for substantive purposes, or created for functional purposes in maintaining the technology, such as processing and structurally organizing the record.\footnote{106} Note that on the Federal Freedom of Information website, there is no discussion or guidance in making requests for metadata or other specific electronic information, such as video or database information.\footnote{107}

In 2014, the Maryland Public Information Act provided clarity through a statutory definition of metadata, which primarily permits disclosure of substantive but not functional metadata:\footnote{108}

"Metadata" defined

(a)(1) In this section, “metadata” means information, generally not visible when an electronic document is printed, describing the history, tracking, or management of the electronic document, including information about data in the electronic document that describes how, when, and by whom the data is collected, created, accessed, or modified and how the data is formatted.

(2) “Metadata” does not include:

(i) a spreadsheet formula;

(ii) a database field;

(iii) an externally or internally linked file; or

(iv) a reference to an external file or a hyperlink.

\footnote{106. See, e.g., Contextual Metadata in the AQUASTAT Database, AQUASTAT (July 2014), http://www.fao.org/nr/water/aquastat/catalogues/MD_in_AQUASTAT_DB_20140707.pdf. While metadata classification schemes change depending on what standards are being used, there are generally two types of metadata: “That which helps you find/identify something”, and “that which helps you understand more about something” [i.e., descriptive metadata]. \textit{Id.}}


\footnote{108. MD. CODE ANN. § 4-205 (2014) (adopted by the State legislature on Oct. 1, 2014).}
However, Maryland’s new statutory definition section also permits a request for information in an electronic format which could include the electronic functionality of the original database.\textsuperscript{109}

\textit{Public record in electronic format}

(c)(1) Except as provided in paragraph (2) of this subsection, the custodian of a public record shall provide an applicant with a copy of the public record in a searchable and analyzable electronic format if:

(i) the public record is in a searchable and analyzable electronic format;

(ii) the applicant requests a copy of the public record in a searchable and analyzable electronic format; and

(iii) the custodian is able to provide a copy of the public record, in whole or in part, in a searchable and analyzable electronic format that does not disclose:

1. confidential or protected information for which the custodian is required to deny inspection in accordance with Subtitle 3, Parts I through III of this title; or

2. information for which a custodian has chosen to deny inspection in accordance with Subtitle 3, Part IV of this title.

While this latter section regarding provision of electronically formatted public records remains relatively vague, particularly regarding the discretion accorded the custodian in determining whether redaction will be too cumbersome, it does provide more guidance than most states have with respect to requests for metadata.

Without statutory guidance, state jurisdictions have been forced to creatively define metadata in a public records context by analogizing to other forms of records and looking to extrajurisdictional opinions and non-legal policy recommendations, such as the Sedona Conference documents.\textsuperscript{110} In the alternative, States may put the burden on the requestor to specifically explain the scope of the database and type of metadata requested,\textsuperscript{111} which is no easy feat for the ordinary citizen. Even when they attempt this, there is no guarantee without statutory guidance that the Court will agree that the request was clear, as was the

\textsuperscript{109} Id. (emphasis added).


\textsuperscript{111} See, e.g., Maese v. Davis Cnty, 273 P.3d 949, 951 n.3 (Utah Ct. App. 2012) (“Maese does not describe the metadata that he asserts is a component of the Redi-Web database.”).
In Maese v. Davis County, the requestor sought “a copy of: [t]he property transaction database, in the electronic format that Davis County keeps it, in its entirety.” And yet the Court bickered with whether this language was a request was for a copy of “the database itself.”

The Sedona Conference Cooperation Proclamation has attempted to provide guidance in defining metadata in the context of civil discovery. It defines metadata in broadly as follows:

10.2.4. A second and more contentious issue arises from requests that seek a form that incorporates “metadata.” Metadata refers to ESI [electronically stored information] that is not apparent from the face of a given electronic “document” and may reveal, for example:

10.2.4.1. date of creation, edits, comments
10.2.4.2. file size and location
10.2.4.3. deletion dates and times
10.2.4.4. access and distribution
10.2.4.5. authorship or the username associated with those tasks

10.2.5. Metadata may show the history of a backdated document or a party’s improper attempts to delete relevant ESI. Thus, there are circumstances under which metadata may be highly relevant. Metadata also provides a means by which a party can conduct a meaningful and relatively inexpensive search of an adversary’s ESI. While the metadata itself may not be relevant to any claim or defense in a particular action, some types of metadata serve a useful purpose in helping the parties access and review relevant ESI.

10.2.6. A responding party may produce ESI in a form that is not in a “reasonably useable form” as required by the rule. This may be because the ESI has been produced in an unusual or proprietary format requiring specialized software to be searched or read, or in a jumbled and disorganized fashion, or in such large volume as to frustrate any effective review. This may be the result of the parties failing to meet-and-confer on the appropriate format prior to production, a failure of

113. Id. at 950.
114. Id. at 951; see Meltzer, supra note 102 (explaining how the Court did not reach the question, as the requestor sought alternative formats).
115. See The Sedona Conference Cooperation Proclamation, SEDONA CONF., https://thesedonaconference.org/cooperation-proclamation (last updated May 2014); see also Blake A. Klinkner, Metadata Redux: Now You’re Telling Me I Need to Provide Metadata to the Opposing Side?, 37 WYO. LAW. 44 (June 2014) (providing a brief history of the judicial development addressing exchange of metadata in civil discovery).
the requesting party to understand the consequences of its request, or an intentional effort by the responding party to hide the ball.

The Sedona Conference guidelines note that Fed. R. Civ. Proc. 34(b)(2)(E)(i) directs that a “party must produce documents as they are kept in the usual course of business or must organize and label them to correspond with the categories in the request . . . . “ Fed. R. Civ. Proc. 34(a)(1)(A) also permits the discovery of “any documents or electronically stored information . . . after translation by the responding party into a reasonably usable form . . . .” Of course, metadata is not necessarily created with the expectation that it will be subject to production in discovery or disclosed pursuant to a public records request. In fact, some have criticized the drawing of parallels between access to metadata in discovery and in a Sunshine Law context.\textsuperscript{117} Ensuring government transparency arguably casts a broader net, where a public records request need not justify the reason for the request, while a civil discovery request is reasonably tailored to the specific purpose of a particular cause of action. It follows then, that courts have shown greater reluctance over time to broadly permit discovery requests for all metadata,\textsuperscript{118} while in contrast, courts increasingly contemplate allowing access to metadata in public records requests.

When a public records request asks for particular information, the requestor may or may not be concerned with how the information is kept “in the usual course of business,” but may be more interested in accessing the information in a particular configuration through use of the database software and search capabilities. The government, of course, is permitted under most public records laws to consider whether compliance with the request allows for a “reasonably usable form” similar to the discovery laws, and permits the government to refuse to create a whole new record in order to comply with the request.\textsuperscript{119} On a practical level, government bodies collecting and storing electronic information subject to potential public records requests would do well to deliberately organize metadata and databases in a form that is efficiently disclosed upon request, and which consistently protects and redacts information subject to exclusion from public records laws.\textsuperscript{120} Custodians of public records are indeed beginning to become more familiar with efficient means of achieving this as

\begin{thebibliography}{120}

\bibitem{117} Meltzer, supra note 102, at 338.
\bibitem{118} Klinkner, supra note 110, at 45 (explaining that “modern courts generally have a presumption against the production of metadata” because most metadata is not likely to produce relevant evidence) (internal citation omitted).
\bibitem{119} See, e.g., Utah Code Ann. § 63G-2-201(12) (“[A] governmental entity shall provide access to an electronic copy of a record in lieu of providing access to its paper equivalent if: . . . (b) the governmental entity currently maintains the record in an electronic format that is reproducible and may be provided without reformattin or conversion;”); see also Maese v. Davis. Cnty, 273 P.3d 949, 952 n.5 (Utah Ct. App. 2012).
\bibitem{120} See David W. Degnan, Accessing Arizona’s Government: Open Records Requests for Metadata and Other Electronically Stored Information After Lake v. City of Phoenix, 3 Phoenix L. Rev. 69, 96 (2010).
\end{thebibliography}
redaction software is incorporated into government database management systems.\textsuperscript{121}

In its simplest context, metadata could be seen to create three-dimensional information, with a choice of seeing a single data point linearly as it relates to other data points (e.g., a single patient name in relation to other patient names in the database), or seeing the single data point in greater depth, not immediately observable when the report is printed (e.g., the time stamp when the name was entered or whether the database has an automatic anonymous numbering system generated for patient names). Electronic information and its metadata, particularly in large databases, thus may provide government with a greater capacity to both share information and to hide information not only because it is voluminous, but because it is like a prism that can be viewed differently as it is turned in different ways.

Keep in mind that the structure of metadata as a deeper layer of information does not inherently define whether the information in a database is substantive or merely functional. The standard colloquial definition of metadata as “data about data” is thus insufficient for legal purposes. The hidden metadata may be substantive, such as the authorship of a document or a history of edits; or merely functional to the workings of the electronic record, such as the instructions for tab settings or size of font. Metadata may also be defined even more specifically, such as linked disparate metadata,\textsuperscript{122} or project boundary metadata,\textsuperscript{123} or system and embedded metadata.\textsuperscript{124} How legislatures choose to define it will impact public records access and whether metadata constitutes “documentary material”, the basic term often used to define a public record.\textsuperscript{125}

Therefore, public records requests simply for “metadata” are likely to be overbroad and ambiguous. It would be as if one would request a copy of paper public records and all that hold them, which may include manila file folders with added pertinent information written on them or the file cabinet itself and its mechanical parts. To leave up to the discretion of the clerk and government agency which metadata are to be produced does not comport with the purpose of a Sunshine Law, which is to grant a right of access to public information regarding the functions of government. Ideally, the agency needs to be informed by the legislature as was accomplished in Maryland,\textsuperscript{126} and the public needs to be

\textsuperscript{121} E.g., Comptroller of Treasury v. Immanuel, 85 A.3d 878, 883 (Md. Ct. Spec. App. 2014) (noting that information from a database can “for a price” be “extracted, sorted and produced,” and this process does not create a new public record which would justify a denial of the public records request).


\textsuperscript{124} Meltzer, supra note 102, at 333.

\textsuperscript{125} See supra note 40 (defining public record in N.C. Gen. Stat. § 132-1).

\textsuperscript{126} See Immanuel, 85 A.3d at 87; see also Brief for The News & Observer Pub. Co. et al., as Amici Curiae Supporting Respondents, LexisNexis Risk Data Mgmt., Inc. v. North Carolina
informed by the agency, on how to make an appropriately specific public records request for metadata in electronic records.

With a continued paucity of appellate decisions and statutory guidance at the state level, both the government and legal profession are notably late to the game in acknowledging the definitional ambiguity of the term “metadata” in public records requests. The tone of the existing opinions tends to reflect pride that the courts now have the ability to address newer technology. Yet other fields also working in the realm of large databases and electronic information have grasped the technology and noted the challenges for more than a decade. For example, in 2001, a researcher on library cataloguing noted:

> When discussed in a Web context, the term “metadata” can refer to either type: the tagging system that defines a set of fields and its contents, or the contents of certain fields that act as descriptors for other resources. This duality can create confusion and it doesn’t help that the same string of characters can act as metadata on one level, and data on another, depending on the perspective being used.127

More than ten years later, we are seeing government departments concerned with the inadvertent release of public records metadata, but providing only basic instructions to address it.128 The fear of governmental secrecy through metadata manipulation has inspired some in the legal profession to simply espouse a policy of deliberate and generalized inclusion of metadata accessible through public records requests.129 Again, the government would do better to simply educate those requesting information.130 A cogent example is that seen on the website for the Presidential Records Act, which helps the public understand its right to request inspection of descriptive metadata or authenticity metadata.131 It is not in the public’s interest to overburden government staff, and it is certainly not in the public’s interest to have the government divulge private and sensitive data inadvertently, or arbitrarily refuse disclosure of important public records within


128. E.g., Guidelines for Editing Metadata, D.N.J., http://www.njd.uscourts.gov/sites/njd/files/EditMetaDataGuidePublic.pdf (last visited Aug. 8, 2015) (focusing on revision metadata and file description metadata). Ironically, that as this resource is in PDF format, its file description metadata appears to be scrubbed, where properties metadata failed to identify the creation date or author.


130. This is already done, for example, by the Federal court system providing a metadata scrubbing instruction handout to assist attorneys working in Federal district court. See Removing Metadata and Hidden Information From Your Document, S.D. Il., http://www.ilsd.uscourts.gov/documents/MetaDataRemoval.pdf (last visited Aug. 9, 2015).

databases and their metadata. Finally, although statutory definitions of metadata and other forms of electronic information beg constant revision in an era of rapid technological change, legislative definitions may provide the best solution to ensure compliance with Sunshine laws in a digital age.

3. Access to Multiple Formats for a Single Public Records Request

In addition, as the public and agencies become accustomed to providing public access to records through online databases, it calls into question whether older methods of recordkeeping, such as microfiche and paper records, will be deemed formats “sufficiently available” as a public record. For example, in *REO Properties Corp. v. Smith*, a county’s hard copy records of property titles had been destroyed after returning the records to Raleigh in the form of microfilm. The North Carolina Court of Appeals held that the absence of an easier format to access records will not excuse a thorough title search, or permit a party to argue that a record is no longer a public record with impact on ownership rights. The North Carolina State Archives electronic public microfilm records in Raleigh, or the County’s own microfilm records, provided sufficiently available public access to *lis pendens* public records in this case, despite the appellant’s contention that microfilm was more akin to a “private cache” than an accessible public record.

Conversely, providing a paper copy of an electronic public record has been recognized as potentially noncompliant by many courts, where metadata containing significant material is missing when printed in hard copy but visible on screen. In their jointly filed amicus brief for the North Carolina Supreme Court review of *LexisNexis*, several media interests have highlighted a key practical difference between obtaining a copy of larger amounts of data frozen in time versus remote access to more limited information on the government database:

> Moreover, remote access to ACIS is qualitatively and substantively different from having a copy of the database. The ACIS database is updated daily (Complaint, ¶25, R p 9-10; Ans. ¶25, R p 33); accordingly, queries entered via remote access tap into the most current data available, but users do not gain access to the complete database. By contrast, the copy of the database that the plaintiffs requested would provide them with a complete “snapshot” of its contents, albeit one that would become out of date rapidly. Regardless of the benefits or deficiencies of one form or medium versus another, the Public Records

---

133. Id. at 235.
134. Id.
Law permits a requester to ask for a record in whatever form or medium most suits its needs.\textsuperscript{136}

The North Carolina Supreme Court in its opinion also noted in \textit{LexisNexis} the difference between requesting records within a database and requesting the database itself:

[T]he information in ACIS both duplicates the physical records maintained by each Clerk and constitutes the collective compilation of all records individually entered by the one hundred Clerks of Court. ACIS includes information not subject to disclosure, and not every employee in each Clerk’s office can access all the information in ACIS.\textsuperscript{137}

Note that a custodian of record may not decline to produce public records in a database simply because the information is also available elsewhere. According to the North Carolina Court of Appeals: “The plain language of the [North Carolina Public Records] Act requires custodians to provide copies of their public records and nothing in the Act suggests that this requirement is obviated because the information contained in a public record is publicly available from some other source. Many public records contain information that is derived from and/or contained in other public records.”\textsuperscript{138} Even if the same information is available in multiple records, a database has the ability to collate and reorganize the information so that its very context creates a potentially new and distinct public record, such as a comparative chart or chronology rather than data points in isolation. This modern ability to reorganize large collections of electronic information has the potential to increase government transparency and decrease the risk of corruption, but risks of overreaching naturally arise.

\textbf{B. Limiting Public Access to Public Records to Protect Government Rather Than Individual Privacy}

Limiting public access to government records for the purpose of protecting public privacy is apparent in the myriad exemptions and exceptions to various public records laws. However, as commercial and private interests seek greater access to the mass collections of information on private individuals maintained in government databases, it appears that the initial legislative approach to curtail overreaching has primarily had the government’s interest in mind, rather than the privacy interests of the individuals whose lives are the subject of the records.

\begin{footnotesize}
\begin{itemize}
\item \textsuperscript{137} \textit{LexisNexis}, supra note 1, at *1.
\item \textsuperscript{138} \textit{LexisNexis (Ct App)}, supra note 76, at 227-28 (emphasis in original). See also \textit{LexisNexis} at *6 (“Access to the public information maintained in ACIS remains fully available by obtaining the physical records from the appropriate Clerk of Court, through the “green screen” terminal maintained in the local courthouse, or by means of a contract with the AOC for remote access.”).
\end{itemize}
\end{footnotesize}
1. A New Exemption for Proprietary Database Computer Code

One possibility of overreaching through requests for public records in databases relates to requesting the computer code creating the software for the database. In 2013, the North Carolina General Assembly enacted an amendment to General Statutes section 132-1.1, providing that the proprietary computer code of government databases is excluded from the definition of a public record. In the absence of contrary authority in *LexisNexis*, with this statutory amendment, a public records request may be made for a copy of the information in an entire government database, excluding the proprietary computer code creating the database. Note that the lower court decision reviewed by the Court of Appeals in *LexisNexis* occurred in February 2013, four months before the North Carolina General Assembly explicitly created a public records exclusion for database computer code in North Carolina General Statutes section 132-1.1.

In *Hearst Corp. v. State of New York*, the New York Supreme Court similarly held that proprietary computer code was not accessible through public records requests for metadata related to a table of employee payroll data because of trade secret protections and risks to the ongoing security of the government database. The affidavit of the Oracle executive was quoted by the court, specifically explaining why it was proprietary:

> PeopleSoft HCM ... includes confidential and proprietary information in the Application Designer portion of the software. The record layouts and electronic fields in the Application Designer function like a blueprint, revealing the architecture of the PeopleSoft software and how it is stored in the database. There are thousands of separate pages in the PeopleSoft HCM Application Designer, all of which contain proprietary information. These record layouts and electronic fields are not available publicly; only licensees of PeopleSoft HCM are able to access them, and Oracle vigorously protects the confidentiality of this information.

As a compromise, the Court did require the government to collect the information within the tables and place it into an electronic spreadsheet as a means of restricting access to the code. Nevertheless, as discussed above, providing a spreadsheet or print out of information is not the same as gaining access to the proprietary code.

---

139. N.C. S.L. 2013-96 (H.B. 125) (“An Act to Clarify that Certain Types of Proprietary Computer Code are not a Public Record.”) (adding N.C. Gen. Stat. § 132-1.1(g)) (enacted June 12, 2013). The provision states, without further defining its terms: “Proprietary computer code written by and for use by an agency of North Carolina government or its subdivisions is not a public record as defined in G.S. 132-1.” *Id.*

140. See generally supra note 95.


142. *Id.* at 877.

143. *Id.* at 878.
access to the database and its metadata and code, which would provide access to all of its internal functions and relational information.\textsuperscript{144}

2. A Traditional Limit on Voluminous Records Requests

Recognition of the need for legislative action to address the financial burden for requests for voluminous electronic public records has been a source of restricting otherwise available public records for many decades.\textsuperscript{145} For example, with regard to \textit{Lake v. City of Phoenix}, which required compliance with a public records request for metadata, one author asserted:\textsuperscript{146}

\begin{quote}
[T]he [Arizona] legislature should define its rules in a manner that produces expected results. In open records law, there is little to stop records from being produced in a harassing manner or from a requesting party from significantly overburdening the government, aside from the proportionality test outlined in the Carlson case, as a public record has a presumption in favor of production. There needs to be some mechanism to determine what open records requests are reasonable, especially as more and more information is stored on the computer without the user’s knowledge.
\end{quote}

Charging reasonable fees or extending time restrictions for production have provided a workable compromise for government compliance with potentially voluminous or complex electronic records requests for some time.

For example, in the late 1980s and early 1990s, Florida sought to ensure continued open records access in a Digital Age through statutorily set fees for certain requests involving remote access, better processes for redaction of confidential information, and copyrighting of computer software maintaining public records databases.\textsuperscript{147} What a reasonable fee would look like for obtaining a properly redacted copy of an entire, complex government database as a public record is debatable. In \textit{Johnson v. Broussard}, the parties gave the trial court

\begin{quote}
\textsuperscript{145} See, \textit{e.g.}, \textit{FAQ – Freedom of Information Law}, N.Y. DEP’T ST., http://www.dos.ny.gov/coog/freedomfaq.html#howmuch (last visited Mar. 22, 2015) (“If you request a large volume of electronic records, the agency can charge the actual cost of reproducing the records. When it takes an agency more than 2 hours to prepare, extract or generate electronic data, the agency could charge for the employee’s time.”); \textit{id.} (citing N.Y. Pub. Off. Law § 87(1)(b)-(c) (McKinney 2014)).
\textsuperscript{147} See Peterson, \textit{supra} note 130, at 447-48; \textit{cf.} Jean Maneke, \textit{The Sun Shines a Little Brighter: Changes to Chapter 610}, 55 J. MO. BAR. 22 (1999) (identifying Missouri as one of the first states to enact Sunshine Laws in 1973, but eventually needing to amend its provisions to address substantially greater amounts of information collected by the government through computers technology).
estimates ranging from $400 to $4,200 to compensate for the government’s expense in redacting confidential information before complying with a complex public records request involving portions of a government database.\textsuperscript{148} The trial court ordered reimbursement up to $500.\textsuperscript{149} In \textit{Johnson}, the Louisiana Court of Appeals held that the costs and time did not preclude compliance with the public records request, and ordered the requestor to reimburse the state in an amount between $500 and $4,200.\textsuperscript{150}

One ramification of the need for more clarity in defining electronic information as a public record is that requests for large amounts of information (as in requests for a whole database or all metadata) risk rejection on the basis of vagueness.

Requests which are worded too broadly or are too all inclusive of a general topic function like a giant broom, sweeping everything in their path, useful or not. They require the respondent either to guess or move through mental gymnastics which are unreasonably time-consuming and burdensome to determine which of many pieces of paper may conceivably contain some detail, either obvious or hidden, within the scope of the request. The court does not find that reasonable discovery contemplates that kind of wasteful effort.\textsuperscript{151}

However, objections regarding volume alone will not generally permit a government to completely deny a request on the basis of unreasonableness. “A record’s length, standing alone, is an insufficient reason to exempt it from open records disclosure.”\textsuperscript{152} In upholding this principle, the Kentucky Supreme Court expressed little sympathy for the Department of Corrections faced with an inmate’s request to access “any and every document contained within my file from the front cover to the back.”\textsuperscript{153} Similarly, the Maryland Court of Appeals, like many jurisdictions, will not permit a government agency to deny a public records request requiring database manipulation, as long as the agency can “perform the data extraction and sorting requested within their existing [software] functionality and in the normal course of business.”\textsuperscript{154}

For those who promote automatic inclusion of metadata in response to public records requests, solutions to address confidentiality and unmanageable amounts of information have rested on familiar policies. “Objections relating to the burden or scope of such requests should be handled largely as they would in civil discovery practice, through good faith discussions aimed at tailoring the request

\begin{thebibliography}{9}
\bibitem{nordr} \textit{Id.} at 1258.
\bibitem{nordr} \textit{Id.}
\bibitem{nordr} Carter v. Archdale Police Dep’t., No. 1:13CV613, 2014 WL 1774471, at *1, *5 (M.D.N.C. Dec. 19, 2014) (internal citations omitted) (addressing both public records and discovery requests).
\bibitem{nordr} Commonwealth v. Chestnut, 250 S.W.3d 655, 666 (Ky. 2008).
\bibitem{nordr} \textit{Id.} at 658.
\bibitem{nordr} Comptroller of Treasury v. Immanuel, 216 Md. App. 259, 270 (Md. Ct. Spec. App. 2014) (holding the manipulation did not require the government to create a “new public record”).
\end{thebibliography}
to specific documents or categories of documents and, if necessary, through application to the courts."155 The fees attached to voluminous requests may also assist in manageability, such as the Federal policy related to FOIA public records requests.156

The only decision to address access to metadata in a Federal FOIA request relied in part on the e-discovery rules of negotiating and coordinating access to voluminous electronic records, but the decision was later withdrawn on other grounds.157 The primary criticism is that any efforts to redact confidential, sensitive information, through blocking out information, or the use of a PDF file or other protected format, is bound to be vulnerable to unveiling by sophisticated recipients or hackers.158 In a single day, on August 19, 2014, computer hackers reportedly obtained 4-5 million records from an American hospital system, and Russian hackers stole 1-2 billion passwords.159 “If records requested under FOIA were required to be produced in native format, any confidential information that was redacted by the agency has the possibility of being recovered by an enterprising adversary.”160 Thus, it has been suggested that electronic records (including metadata) should never be produced in native formats, but instead,

---


156. Frequently Asked Questions, FOIA, http://www.foia.gov/faq.html#cost (last updated Feb. 2011) (“For a typical requester the agency can charge for the time it takes to search for records and for duplication of those records. There is usually no charge for the first two hours of search time or for the first 100 pages of duplication.

You may always include in your request letter a specific statement limiting the amount that you are willing to pay in fees. If an agency estimates that the total fees for processing your request will exceed $25, it will notify you in writing of the estimate and offer you an opportunity to narrow your request in order to reduce the fees.

You may request a waiver of fees. Under the FOIA fee waivers are limited to situations in which a requester can show that the disclosure of the requested information is in the public interest because it is likely to contribute significantly to public understanding of the operations and activities of the government and is not primarily in the commercial interest of the requester. Requests for fee waivers from individuals who are seeking records pertaining to themselves usually do not meet this standard. In addition, a requester’s inability to pay fees is not a legal basis for granting a fee waiver.”).


158. Id.


160. Meltzer, supra note 150, at 348.
should be printed out in hard copy. As discussed below, in the most sensitive and stigmatized realms of criminal justice and public health, those with authority to address public records policies, judicial interpretation, and statutory reform should take heed, for ignoring or minimizing the risks to government security and individual privacy rights through disclosure of entire databases is naïve at best.

III. EXPLORING THE EXPANDING FRONTIER: REVERSE SUNSHINE FOR THE “GREATER GOOD”?

In the name of public safety and the “greater good”, criminal justice records have consistently formed the experimental front in the trend toward public database creation and expanded disclosure of personal information as a matter of public record. The criminal justice system in amassing such information electronically balances the interests of safety and privacy of defendants, crime victims, witnesses, and the public at large. Similarly, public health records also require a crucial balance of interests, such as the safety and privacy of patients versus the need to inform the public of health risks. In both the criminal justice and public health systems, there exists the important public policy goal of providing public notice, as well as, government transparency to ensure that the government is responding appropriately to important health and safety matters.

As will be shown below, the familiarity with criminal databases and registries on offenders has influenced the expansion of public health databases and mass surveillance. Most begin as exempt from public records categories, but a clear trend shows a tendency for state and federal legislatures to eventually acquiesce to the request of government to make more and more databases public; that is, databases that share personal information on individuals. In turn, other areas of government in which large collections of personal information are stored may be increasingly subject to public records requests. Indeed, LexisNexis involved a request for an electronic copy of ACIS, a database of the criminal records of offenders. If the North Carolina Supreme Court affirms the Court of Appeals determination that the public records statute permits such access, then the door is open in that State for requests for copies of a myriad of criminal and non-criminal government databases.

A. The Criminal Justice System: The First Wave of Reverse Sunshine Disclosing Personal Information by the Government

Government records compiling information on individuals in databases and registries often consist of mandatory collections of information from individuals. Criminal defendants are the focus of some of the most aggressive
Prisoners witness their identities, images and other personal information transformed into matters of public record, displayed in multiple state and Federal criminal registries and databases, made available to the globe online. While the authorized infringement on personal privacy of offenders may have begun with the convicted and incarcerated, it has eventually expanded to those who are not guilty, as seen in DNA databases of the arrested and familial investigative searches. To avoid being caught in the expanding web of criminal justice system public records, the crime victim rights movement has fought for increasing concealment of what otherwise would be the public information of crime victims as witnesses in public record.

1. An Early Focus on Use of Public Databases to Address Recidivism

The curtailment of the privacy and liberty interests of the incarcerated is most often justified when directed at violent recidivist offenders, such as sex offenders and domestic violence batterers who pose a higher risk to public safety, despite the fact that burglary is the highest recidivist crime. Technological advances also tend to justify new efforts in surveillance of criminals in public, such as GPS monitoring of criminal offenders. Would the next violent

---

164. See, e.g., Mary D. Fan, Constitutionalizing Informational Privacy by Assumption, 14 U. PA. J. CONST. L. 953, 985-86 (2012) (discussing both informational privacy right and 8th Amendment cruel and unusual punishment violations for unwarranted disclosure of private medical information of prisoners).

165. See, e.g., Identity History Summary Checks, Fbi, http://www.fbi.gov/about-us/cjis/identity-history-summary-checks/ (last visited Mar. 22, 2015) (providing access to a person’s own Identity History Summary, with the submission to the FBI or its third party processing contractor (an “FBI-approved Channeler”) of the person’s fingerprints and social security number).


168. See Matthew R. Durose, Alexia D. Cooper, & Howard N. Snyder, Recidivism of Prisoners Released in 30 States in 2005: Patterns From 2005 to 2010, DOJ (Apr. 2014), http://www.bjs.gov/content/pub/pdf/rprts05p0510.pdf (“Within 5 years of release, 82.1% of property offenders were arrested for a new crime, compared to 76.9% of drug offenders, 73.6% of public order offenders, and 71.3% of violent offenders.”).

169. See Nat’l Inst. Of Justice, Electronic Monitoring Reduces Recidivism, DOJ (Sept. 2011) https://www.ncjrs.gov/pdffiles1/nij/233446.pdf; see also Scott McCallum & Brian Barton, GPS Offender Monitoring and Tracking, Pinellas County, Florida/Marion County, NCJRS, https://www.ncjrs.gov/pdffiles1/nij/gps-offender-monitoring.pdf (last visited Mar. 22, 2015) (indicating [as of 2006] GPS is most commonly used to track sex offenders, but some states are using GPS to monitor other high-risk offenders. For example, New Jersey and California are contemplating GPS monitoring in domestic violence cases; Delaware uses GPS to track movements
offender registry track movement through live-streaming for public monitoring online, a method arguably helpful to victims of stalking, for example. While this may seem fanciful, it is important to look at the trend of expansion of government collection of personal information and dissemination for its own uses and that of public record. There has been no parallel movement with equal force in the opposite direction toward respect for privacy, or restriction on mass collection practices. The future advances in information collection and storage technology will likely continue to seduce government and commercial interests, but require ardent attention to the interests of individual privacy.

Below is a chronological selection of some of the State and Federal criminal registries and databases consisting of public and exempt Federal records, including a focus on North Carolina, the State in which LexisNexis was recently decided. Note that across the United States, many other types of crimes have formed the basis of new offender registries, with some debate, such as those related to domestic violence, murder, animal abuse, driving while intoxicated (DWI), and general violent crimes. None has made information public and then retracted access as a matter of public policy and defendant’s rights. Moreover, public records access to these criminal justice system databases continues to expand. The most recent expansion by the U.S. Department of Justice, granting access to an array of federal criminal databases to federally-recognized tribes was touted by the department: “It is our hope that TAP can minimize the national crime information gap and drive a deeper and more meaningful collaboration between the federal, state, local and tribal criminal justice communities. . . .”

of juveniles under house arrest; and Pasco County, Florida, is using GPS for pretrial inmates to reduce jail overcrowding).

170. See generally STEVEN JOHNSON, MIND WIDE OPEN: YOUR BRAIN & THE NEUROSCIENCE OF EVERYDAY LIFE (2004) (noting that neuroscientific technology may now allow for use of MRI imaging and other brain mapping and tracking methods to allow us to transmit thoughts and choices directly into computers, or to detect truthfulness and employment aptitudes with greater accuracy. If these images and messages are recordable, in future one could envision creating government thought registries of those more apt to commit crime or betray the public trust).

171. See supra Section III(A)(1).


174. Id. (proposed in Pennsylvania in 2014).


176. Id. (Montana and Oklahoma).

# Chronology of Criminal Justice Databases and Registries

<table>
<thead>
<tr>
<th>DATE</th>
<th>TITLE AND AUTHORITY</th>
<th>OFFENDER FOCUS</th>
<th>PUBLIC RECORD</th>
</tr>
</thead>
<tbody>
<tr>
<td>1947</td>
<td>Megan’s Law in California[^178]</td>
<td>First state to have a sex offender registry</td>
<td>Not until 1997 in person at police stations; 2004 online</td>
</tr>
<tr>
<td>1967</td>
<td>National Crime Information Center (NCIC)[^179]</td>
<td>Clearinghouse (now electronic) of crime data accessible to all law enforcement</td>
<td>No</td>
</tr>
<tr>
<td>1986</td>
<td>NC Statewide Automated Fingerprint Identification System (SAFIS)[^180]</td>
<td>First electronic database of fingerprints used in criminal investigations</td>
<td>No</td>
</tr>
<tr>
<td>1990</td>
<td>Washington[^181]</td>
<td>First state to provide public notice of sex offender registry status</td>
<td>Yes</td>
</tr>
<tr>
<td>1993</td>
<td>National Instant Criminal Background Check System (NICS)[^182]</td>
<td>Database screening tool to determine if a person is legally prohibited from purchasing a firearm</td>
<td>Partially</td>
</tr>
<tr>
<td>1993</td>
<td>NC Combined DNA Index</td>
<td>First database collection of statewide DNA from</td>
<td>No</td>
</tr>
</tbody>
</table>


[^181]: See State v. Ward, 869 P.2d 1062, 1065 (Wash. 1994) (describing the history of the enactment of the statutory authority for Washington’s sex offender registry); see also Catherine L. Carpenter & Amy E. Beverlin, The Evolution of Unconstitutionality in Sex Offender Registration Laws, 63 Hastings L.J. 1071, 1093 (2012) (“[C]ourts [have] declared [sex offender] community notification statutes constitutional because, on balance, the collected data were disseminated in a controlled manner and contained no more information than what is otherwise disseminated by the fact of conviction.”).

<table>
<thead>
<tr>
<th>DATE</th>
<th>TITLE AND AUTHORITY</th>
<th>OFFENDER FOCUS</th>
<th>PUBLIC RECORD</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>System (CODIS)(^{183}) N.C. Gen. Statutes Chapter 15A</td>
<td>convicted criminal offenders</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Jacob Wetterling Crimes Against Children &amp; Sexually Violent Offender Act 42 U.S.C. § 14071</td>
<td>First requires states to implement a sex offender registry to receive certain Federal law enforcement funds</td>
<td>Not initially, but states varied; mandated public notice by 1996</td>
</tr>
<tr>
<td>1995</td>
<td>Firearm Inquiry Statistics Project(^{184})</td>
<td>Federal collection and publication of annual data on presale firearm inquiries under the Brady Act</td>
<td>Yes</td>
</tr>
<tr>
<td>1996</td>
<td>NC Sex Offender &amp; Protection Registry(^{185})</td>
<td>First NC sex offender registry</td>
<td>Yes</td>
</tr>
<tr>
<td>1997</td>
<td>National Registry of Protective Orders(^{186})</td>
<td>National compilation of State and Federal domestic violence and stalking protective orders</td>
<td>No</td>
</tr>
<tr>
<td>1998</td>
<td>FBI Combined DNA Index System (CODIS) 42 U.S.C. § 14132</td>
<td>Federal system combining national, state, and local laboratory investigative DNA records</td>
<td>No</td>
</tr>
<tr>
<td>2006</td>
<td>Adam Walsh</td>
<td>Expansion of Federal and</td>
<td>Yes</td>
</tr>
</tbody>
</table>

---


<table>
<thead>
<tr>
<th>DATE</th>
<th>TITLE AND AUTHORITY</th>
<th>OFFENDER FOCUS</th>
<th>PUBLIC RECORD</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Child Protection &amp; Safety Act (SORNA) 187 42 U.S.C. 16911</td>
<td>state sex offender registries and new national registry 188 including juveniles (14 and older), publicly disclosing home, school, and work addresses</td>
<td></td>
</tr>
<tr>
<td>2006</td>
<td>CA Jessica’s Law 189</td>
<td>First lifetime GPS monitoring of sex offenders and predator-free zones</td>
<td>Yes</td>
</tr>
<tr>
<td>2007</td>
<td>NC Jessica’s Law 190 N.C. Gen. Stat. § 14-208.40A et seq.</td>
<td>GPS lifetime monitoring of sex offenders, and expanding the registry definition of sexual offense</td>
<td>Yes</td>
</tr>
<tr>
<td>2008</td>
<td>KIDS Act (Keeping the Internet Devoid of Sexual Predators Act), amending Adam Walsh Act 42 U.S.C. § 16911</td>
<td>Requiring convicted sex offenders to register their email addresses with the National Sex Offender Registry, and enabling social networking sites to voluntarily search the registry for misuse</td>
<td>Partially</td>
</tr>
<tr>
<td>2008</td>
<td>NC SAFIS comprehensive update 191</td>
<td>Statewide fingerprint database transferred to digitized records and live-scanning of prints</td>
<td>No</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>DATE</th>
<th>TITLE AND AUTHORITY</th>
<th>OFFENDER FOCUS</th>
<th>PUBLIC RECORD</th>
</tr>
</thead>
<tbody>
<tr>
<td>2009</td>
<td>Adam Walsh Act deadline(^\text{192})</td>
<td>Requiring states to include juveniles in the public sex offender registries (14 and older)</td>
<td>Discretionary(^\text{193})</td>
</tr>
<tr>
<td>2010</td>
<td>NC CODIS expansion N.C. Gen. Stat. § 15A-266.3A</td>
<td>Expands collection of investigative DNA from persons arrested but not convicted of certain offenses</td>
<td>No</td>
</tr>
<tr>
<td>2015</td>
<td>Tribal Access Program for National Crime Information (TAP)(^\text{194})</td>
<td>Grants access to federally-recognized tribes to national crime information databases for civil and criminal purposes</td>
<td>Unspecified</td>
</tr>
<tr>
<td>Ongoing</td>
<td>National Criminal Justice Data Improvement Program(^\text{195})</td>
<td>Improving criminal record-keeping of State and local government to automatically interface their databases with Federal databases</td>
<td>Some</td>
</tr>
<tr>
<td>Currently</td>
<td>NC Automated System Query (ASQ), Dept. of Public Safety(^\text{196})</td>
<td>Combines State criminal justice system databases to permit online customized information queries</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Some of the criminal public databases expressly exempt certain information for reasons related to violation of internal policies or other law. The *Sex Offender Registration and Notification Act*, authorized by Title I of the Adam

---

193. See N.C. GEN. STAT. § 14-208.29 (exempting juveniles from public notification requirements).
Walsh Child Protection and Safety Act of 2006 (SORNA), created the following mandatory exemptions for certain information that would not be placed on the internet as public record, although still required to be submitted to the registry for law enforcement use: (1) identity of the sex offense victim; (2) offender social security number; (3) arrests not resulting in conviction; and (4) any information the Attorney General exempts. In addition, a jurisdiction may opt to exclude from public view the following: (1) information about a tier one sex offender if the offense was not against a minor; (2) the name of an employer of the sex offender; (3) the name of an educational institution where the sex offender is a student; and (4) other information the Attorney General sees fit to exempt.\footnote{197}

In North Carolina, the Attorney General opted not to release into public record the victim’s identity, nor the medical or mental health records or documentation of treatment for the sex offender.\footnote{198} When the North Carolina Supreme Court in \textit{LexisNexis} recently addressed the statutory provision granting potential commercial vendors licenses for remote access to electronic governmental databases,\footnote{199} it did not discuss the reality that such access would require enhanced scrutiny, such as the need for potential scrubbing of confidential or otherwise exempt metadata. The official rationale for making what information is available to the public is stated as follows: “This information is made available for purposes of protecting the public, for increasing awareness, for keeping the public informed and for allowing citizens to take proactive measures to ensure safety in their communities.”\footnote{200} This begs the question whether exemptions relate to offender privacy interests, if they are not helpful to public safety.

In 2013, North Carolina enacted a law that prohibits employers and academic institutions from requesting information about criminal records that have been expunged.\footnote{201} Remember, however, that the Internet has transformed the ability of the public to access more and more information that is public or was public at one time. The North Carolina Free Public Records Directory displays free statewide public record information on the residents of North Carolina, with additional local public information available on county websites.\footnote{202} The site also provides a link to the government sponsored public records website in every other state.


199. See supra Part III.A.1.


Over time it has become concerning that the infringement on the liberty and privacy interests of criminal offenders is not often examined properly when the government registry measures are enacted and reviewed piecemeal. Once enacted, however, these registries tend not to be abandoned as a matter of public policy creating at least an appearance of public protection. For example, in San Diego, California, one of the largest cities in the United States, an online map was created of the “red zones” in which registered sex offenders could not live because they were near public parks, pools, video arcades, libraries, amusement parks, and other areas prohibited to them as defined by state law and city ordinance. It blocked out most of the city.203

In North Carolina, the Attorney General’s Office has developed similar online mapping of “all offenders’ addresses up to five miles away from any site you choose, such as home, school, child care center or park.”204 The North Carolina Attorney General’s Office also offers a Sex Offender mobile app to access the registry more easily on personal devices.205

The justification for public sex offender registries is clear in terms of policy, but short on evidence-based analysis. For example, while half of adult sex offenders report that their sexual offending began in adolescence, there has been little data examining whether a comparable number of juvenile offenders, required to register, are likely to reoffend in the future.206 Some recent data does indicate that juveniles and adults re-offend at similar rates, and those who begin offending as juveniles may be even more likely to re-offend.207 With so many vital safety and privacy interests at stake, the actual efficacy of intrusive governmental action regarding convicted offenders has received surprisingly little public examination, even in light of more recent judicial assumptions of a right to informational privacy.208

Some researchers argue that “[p]ushing sex offenders to the margins of our society, with nothing left to lose, only increases the chance that they will re-offend.”209 Even the statewide victims’ rights group, the California Coalition
Against Sexual Assault, has opposed residency restrictions related to sex offenders based on evidentiary research to date: “Residency restrictions . . . don’t make communities safer. Residency restrictions don’t reduce recidivism, don’t improve supervision of offenders and ultimately do not protect children from sex offenders.”

Patty Wetterling, the mother of the boy who inspired enactment of the 1994 Jacob Wetterling Crimes Against Children & Sexually Violent Offender Act, has gone on record supporting the position of the National Association of Criminal Defense Attorneys, asserting to no avail that the Adam Walsh Act is overbroad and unconstitutional.

The retention of unproven but presumptively “tough on crime” and pro-crime prevention public database access unfortunately redirects focus away from other evidence-based approaches that may work better to prevent serious recidivist violent crime. This critical look at efficacy is even more vital when considering the key role criminal databases have played in setting the stage for expanding public information access into other previously confidential collections of government information outside the realm of criminal justice.

2. The Forgotten Rationale: Moving Beyond Recidivism

The expansion of mass governmental collection and public dissemination of information to prevent criminal offender recidivism has had a tendency to expand into other areas of the criminal justice system, as well as to other non-criminal government systems. The North Carolina Department of Corrections Public Access Information System is an online resource, which provides public information on convicted offenders’ criminal records, data, escapes, captures, and releases in North Carolina, regardless of the type of crime. “Data” includes sentence history, date of birth, gender, race, supervision and inmate status, and docket and DOC numbers. However, the restriction to collection of

---


213. See, e.g., CHARLOTTE GILL ET AL., EVIDENCE-BASED ASSESSMENT OF THE CITY OF SEATTLE’S CRIME PREVENTION PROGRAMS 9 (George Mason Univ. 2012), available at http://cebcp.org/wp-content/evidence-based-policing/seattle-assessment (“Programs should be required to develop measureable and relevant outcomes: crime prevention programs should measure effects on crime as a primary or secondary outcome.”).

information on convicted offenders is merely a matter of history. Today, the
government engages in such practices as mandatory collection of DNA profiles
from arrestees, which remain confidential, and mandatory collection of mental
health and substance abuse treatment information from persons applying for a
gun permit, which has now become a matter of public record.

With respect to governmental collection of DNA, the United States has the
largest DNA databank in the world: “Now, DNA is being collected from felons
in 45 states, from juvenile offenders in 32 states, for misdemeanors in 34 states,
and upon arrest in 12 states. The federal government is encouraging states to
collect and retain DNA of people upon arrest, from people who should be
presumed innocent until proven guilty.”

In North Carolina, for example, DNA is collected from persons arrested, but
not convicted, for the commission or attempt to commit the following crimes:

1. G.S. 14-17, First and Second Degree Murder.
2. G.S. 14-18, Manslaughter.
3. Any offense in Article 7A, Rape and Other Sex Offenses.
4. G.S. 14-32, Felonious assault with deadly weapon with intent to kill
   or inflicting serious injury; G.S. 14-32.4(a), Assault inflicting serious
   bodily injury; G.S. 14-34.2, Assault with a firearm or other deadly
   weapon upon governmental officers or employees, company police
   officers, or campus police officers; G.S. 14-34.5, Assault with a firearm
   on a law enforcement, probation, or parole officer or on a person
   employed at a State or local detention facility; G.S. 14-34.6, Assault or
   affray on a firefighter, an emergency medical technician, medical
   responder, emergency department nurse, or emergency department
   physician; and G.S. 14-34.7, Assault inflicting serious injury on a law
   enforcement, probation, or parole officer or on a person employed at a
   State or local detention facility.
5. Any offense in Article 10, Kidnapping and Abduction, or Article
   10A, Human Trafficking.
6. G.S. 14-51, First and second degree burglary; G.S. 14-53, Breaking
   out of dwelling house burglary; G.S. 14-54.1, Breaking or entering a
   place of religious worship; and G.S. 14-57, Burglary with explosives.
7. Any offense in Article 15, Arson.
8. G.S. 14-87, Armed robbery.
9. Any offense which would require the person to register under the …
   Sex Offender and Public Protection Registration Programs.

215. Sujatha Jesudason, Building a DNA Databank of People of Color, COLORLINES (July 2,
In cold cases, the North Carolina State DNA Database is also authorized to collect DNA from potential victims as well, such as missing persons and relatives of missing persons. The information is not public record at this time, and statutory exemptions from the Public Records Act provide for Class H felony charges for unauthorized disclosure of a person’s DNA profile from the state database. Familial searches, in which partial DNA matches lead investigators to family members in hopes of locating biologically related offenders, is also a tool of the government. To date the expansion of use has been slow, and only California, Colorado, Texas, and Virginia authorized such use, but not at the national level within the National DNA Index System. Yet, much criticism has accompanied this development, as it would disproportionately impact innocent members of low-income families and families of color. As Professor Mnookin of the UCLA School of Law argues:

While we might not be sympathetic to the claim of a privacy violation made by a guilty person caught by familial search techniques, we ought to care that these procedures disproportionately affect the underprivileged.

If it is ethically and legally acceptable to use DNA search techniques on people without prior convictions, then why not have a national database that includes everyone? The misfortune of having a criminal in the family tree ought not to determine who’s included in the database and who’s left out.

219. Michael Chamberlain, Familial DNA Searching: A Proponent’s Perspective, 27 CRIM. JUST. 18, 30 (2012) (“[C]onsidering familial relationships by police is not uncommon in non-DNA investigations of, for example, domestic violence, child abuse, and child sexual assault cases.”).
Keep in mind that the familial DNA analyzed may be already contained within a state’s DNA database, tested without the consent of the innocent family member who may have been arrested or convicted of a crime in the past, or it may be a DNA sample obtained with consent from suspected family members whose DNA is not already in the database. When will it become acceptable to create familial databases for public health concerns including the spouses and dating partners of those who are HIV positive? When will all state employees be required to provide fingerprint or DNA data as a prerequisite to employment? Will existing digital collections of fingerprints, such as that of licensed attorneys, be made available as a matter of public record? When will any of the exemptions to the Public Records Act for such databases disappear so that, in addition to the government, all others on the planet have access to this information? The trend is clear. Those most vulnerable to state intervention and control, such as foster children, enlisted men and women, institutionalized persons with mental illness and other disabilities, and the arrested and incarcerated are most likely to find themselves to be a data point in a government database first.

While medical privacy is highly valued, public health interests continue to serve as a core exception for public records access, particularly those areas of public health that intersect with criminal justice interests. For example, in light of horrific gun violence across the nation, some of which has involved perpetrators who are mentally ill, new legislative measures now allow government access to mental health records as a screening tool for the National Instant Criminal Background Check System (NICS). This database provides law enforcement and commercial sellers of firearms with instant access to such information about a potential purchaser in order to legally bar the sale.

Federal law has also included a history of substance abuse or involuntary commitment as a health-related basis for denying the purchase. However, states are currently not required to disclose their citizens’ mental health records to NICS, thus the database has always been incomplete. After the homicide of 32 students on the Virginia Tech campus in April 2007 by a shooter later

226. Id. (noting the 2007 Virginia Tech shooting involved the sale of a firearm to a person with a documented history of mental illness, whose mental health information had not submitted to NICS).
identified as a mentally ill student, the North Carolina General Assembly introduced companion bills to require the addition of certain mental health records into NICS. The only method of removing or correcting the mental health information from NICS would be for the affected individuals to petition the court, proving they no longer pose a threat to themselves or others. After a denial of petition, the defendant may appeal to a higher court or wait another year before re-petitioning.

In 2013, the North Carolina Legislature passed a law amending state firearm restrictions for issuance or refusal of a gun permit. As a matter of public record, the sheriff is now required to keep a list of persons who have been denied a gun permit and the reasons for which they have been denied. Some of the grounds for denial are matters that would have been protected by other confidentiality laws related to medical and mental health treatment and assessment, including:

(3) One who is an unlawful user of or addicted to marijuana or any depressant, stimulant, or narcotic drug (as defined in 21 U.S.C. § 802).

(4) One who has been adjudicated mentally incompetent or has been committed to any mental institution.

(6) One who has been discharged from the Armed Forces of the United States under dishonorable conditions.

These new public record provisions would not violate confidentiality law, as any person requesting a permit must consent to the disclosure. Any person unwilling to consent to the disclosure need not apply. Note that in addition to the new public record created from the information forming the basis of denial of a permit, the Sheriff is also required by state law to transmit this information to the federal government’s NICS. Therefore, this may be the first North Carolina government database of mental health and substance abuse status made readily available to non-governmental individuals with no interest in providing treatment services for the ill.


228. N.C. GEN. STAT. § 122C-54.1 (2014).

229. Id.


233. See supra notes 64-71 and accompanying text (discussing government databases of voluntarily provided personal information).

Other states are attempting to better control firearms restrictions and reduce gun violence in other ways. For example, in 2014, Maryland proposed a bill to enact legislation to link its firearm ownership database with its state criminal database, and directs law enforcement to conduct door-to-door searches for gun owners who have not relinquished their firearms.\textsuperscript{235} Gun rights advocates denounced this as an infringement of Second Amendment rights, and indicated the inequitable application of the grounds for denial of permits, including mental health evaluations without sufficient evidence.\textsuperscript{236}

Recall that a recent North Carolina judicial interpretation of the Public Records Act addressed whether the entire Automated Criminal/Infraction System (ACIS) database is a single public record subject to a public information request.\textsuperscript{237} The North Carolina Court of Appeals in \textit{LexisNexis} held that the system itself is a public record and that the custodian is the North Carolina Administrative Office of the Courts (AOC), not the individual clerks of court in each county.\textsuperscript{238} Reversing on other grounds, the North Carolina Supreme Court in \textit{LexisNexis} declined to consider who is the custodian of an electronic database.\textsuperscript{239} While the ACIS database addressed by \textit{LexisNexis} is a database of public criminal court records, in North Carolina it now appears more likely that any of the many government databases that evolve from private to public, such as the mental health basis for denial of a gun permit, could be requested as public record as an entire database. The end result is that, thereafter, this mass information collected by the government on its citizens will be potentially disseminated online for the entire world to see in any governmental, commercial or private web platform.

\textbf{B. The Public Health System: The Second Wave of Reverse Sunshine}

The Reverse Sunshine effect seen clearly in the expansion of criminal justice databases containing massive public records of the personal information of individual offenders, has already justified expansion to areas of public health that intersect with criminal justice public safety concerns.\textsuperscript{240} When addressing whether government records are public or private, note that medical records maintained within a Public Records Act that defined agency, have often been

\begin{thebibliography}{9}
\bibitem{235} Paul Joseph Watson, \textit{Showdown: Maryland to Target 110,000 Citizens with Gun Confiscation}, \textsc{Infowars.com} (March 5, 2014), http://www.infowars.com/showdown-maryland-to-target-110000-citizens-with-gun-confiscation/.
\bibitem{236} Id.
\bibitem{237} See supra Part III.A.1.
\bibitem{238} \textit{LexisNexis (Ct App)}, 754 S.E.2d at 228.
\bibitem{239} \textit{LexisNexis}, supra note 1 at *5 (“Because this statute does not refer to the ‘custodian’ of the pertinent records, we need not address arguments that are dependent on a determination of who is the custodian of ACIS and the records included in that database.”).
\bibitem{240} See, \textit{e.g.}, Part IV.A (addressing firearms and mental health databases).
\end{thebibliography}
hybrids of both. The records of government agencies, state-owned hospitals, and even some private nonprofit hospitals and treatment providers under government supervision, would be interpreted as public records within the meaning of the Public Records Act. In addition, many states have determined that no request for records may be denied “on the grounds that confidential information is commingled with the requested non-confidential information,” which requires that agencies bear the cost of separating or redacting information that is exempt from disclosure. Thus, even complex electronic records management systems containing highly sensitive medical information may potentially face public records requests.

1. Protecting Privacy in Public Health Databases

Most statutory exclusions from public records involving health information permit: (1) the patient to access the records, (2) disclosure subject to law enforcement request or court order, and (3) disclosure if personally identifiable information is redacted. For example, the most recent exemption in the North Carolina Public Records Act, that for Eugenics Program records access, is typical of this structured approach:

N.C. GEN. STAT. § 132-1.23 (2014). Eugenics program records

(a) Records in the custody of the State, including those in the custody of the Office of Justice for Sterilization Victims, concerning the Eugenics Board of North Carolina’s program are confidential and are not public records, including the records identifying (i) individuals impacted by the program, (ii) individuals, or their guardians or authorized agents, inquiring about the impact of the program on the individuals, or (iii) individuals, or their guardians or authorized agents, inquiring about the potential impact of the program on others.

241. Since the 1980s, government generated public health and medical and patient databases have expanded to address the perceived “urgent need to understand patterns and trends in the use and cost of medical services in this State.” N.C. Att’y Gen. Opinion 57-38, N.C. DOI (Sept. 24, 1987), available at http://www.ncdoj.gov/About-DOJ/Legal-Services/Legal-Opinions/Opinions/57-38.aspx (addressing the impact of Federal drug treatment confidentiality provisions on the role of the State Medical Database Commission).


243. N.C. GEN. STAT. § 132-6(c) (2014). See also Johnson v. Broussard, 118 So.3d 1249, 1257 (La. Ct. App. 2013) (upholding the trial court determination that a cumbersome redaction process will not justify a denial of a public records request for database information).


(b) Notwithstanding subsection (a) of this section, an individual impacted by the program, or a guardian or authorized agent of that individual, may obtain that individual’s records under the program upon execution of a proper release authorization.

(c) Notwithstanding subsections (a) and (b) of this section, minutes or reports of the Eugenics Board of North Carolina, for which identifying information of the individuals impacted by the program have been redacted, may be released to any person. As used in this subsection, “identifying information” shall include the name, street address, birth day and month, and any other information the State believes may lead to the identity of any individual impacted by the program, or of any relative of an individual impacted by the program.

As a state example, below is a list of certain express exceptions to public records disclosure involving medical and health information in North Carolina, many of which comprise a hybrid approach where some but not all of the records are accessible through a public records request.246 Several exceptions also display the intersection between criminal justice and public health systems, such as those related to records of autopsy, commitment, competency, controlled substance use, and crime victim compensation.

- Adult Care Home inspection records on specific residents and complaints filed with the Department of Human Resources (N.C. Gen. Stat. § 131D-27 (2014)).

- Autopsy photographs and audio recordings subject to inspection, but limited copying access (N.C. Gen. Stat. § 132-1.8 (2014))247; however, the text of an official autopsy report, including any findings and interpretations prepared in accordance with N.C. Gen. Stat. § 130A-389(a) (2014), is a public record and fully accessible by the public. For purposes of this section, an official autopsy is an autopsy performed pursuant to N.C. Gen. Stat. § 130A-389(a) (2014).


---

246. Complied in part from Federal Open Government Guide, REPORTERS COMM. FOR FREEDOM PRESS, http://www.rcfp.org/federal-open-government-guide (last visited May 11, 2015). Note that some of these “health related” public records exceptions also involve the criminal justice system, such as competency evaluations, controlled substance abuse treatment records, and crime victim compensation records. Id.

• Competitive health care information by public health authorities and hospitals (N.C. GEN. STAT. § 130A-45.11 (2014); N.C. GEN. STAT. § 131E-97.3 (2014); N.C. GEN. STAT. § 131E-99 (2014)).

• Controlled substances treatment and rehabilitation (N.C. GEN. STAT. § 90-109.1(a) (2014)).

• Controlled substances research (N.C. GEN. STAT. § 90-113.3(e) (2014)).

• Dental Licensing Board (N.C. GEN. STAT. § 90-41(g) (2014)).

• Dental Peer Review Committees (N.C. GEN. STAT. § 90-48.10 (2014)).

• Health and Medical Records in the possession of the Dept. of Human Resources or local health departments (N.C. GEN. STAT. § 130A-12 (2014) (admission, treatment, discharge); N.C. GEN. STAT. § 131E-97 (2014) (patient charges and accounts); N.C. GEN. STAT. § 130A-374(a) (2014) (permitting patient consent for disclosure)).

• Health care records of teachers and state employees (N.C. GEN. STAT. § 135-48.10 (2014)).

• Health Maintenance Organizations (HMO) patient records (N.C. GEN. STAT. § 58-67-180 (2014)).

• Hospice patient records (N.C. GEN. STAT. § 131E-207 (2014)).

• Inspections of regulated facilities (e.g., N.C. GEN. STAT. § 122C-25 (2014) (mental health); N.C. GEN. STAT. § 131E-150 (2014) (ambulatory surgical)).

• Involuntary commitment court records (N.C. GEN. STAT. § 122C-207 (2014)).

• Medical Database Commission (N.C. GEN. STAT. § 131E-214.3 (2014)).

• Medical Review Committees (N.C. GEN. STAT. § 131E-95 (2014)).

• Nursing home complaints to the Dept. of Human Resources (N.C. GEN. STAT. § 131E-124(c) (2014)).

• Occupational Safety and Health inspections (N.C. GEN. STAT. § 95-152 (2014)).

• Pastoral Counselors (N.C. GEN. STAT. § 90-390(c) (2014)).

• Pharmacy records (N.C. GEN. STAT. § 90-85.36(a) (2014)).

• Physician investigations under the NC Medical Board (N.C. GEN. STAT. § 90-14(d) (2014)).

• Psychologist investigations under the NC Psychology Board (N.C. GEN. STAT. § 90-270.15(e) (2014)).

• Victims Compensation Commission medical records (N.C. GEN. STAT. § 15B-8.1 (2014)).

Sometimes a public health concern invokes the highest levels of police power through civil and criminal regulation, such as firearm regulation, particularly when it overlaps with criminal justice concerns. In the wake of horrific gun violence in the United States, there exists a deep divide in views on how to manage the public health crisis, but all decry the level of violence. Some advocate increased gun restrictions and screening through database sharing to reduce the number of guns available to those who may harm others, while others advocate lessened gun restrictions to increase the number of guns available for self-defense. Creating government records on mental health as a tool for screening gun permit applications is also contentious, as discussed in this news report:

In North Carolina, you have to go through the sheriff to buy a handgun. The New Hanover County Sheriff’s Office runs all applicants through the NICS system - the FBI’s National Instant Background Check Service that includes information on criminal records and involuntary commitments for mental problems.

For concealed carry applicants, the New Hanover County Sheriff’s also does record checks with three local mental health providers: Coastal Care, Wilmington Treatment Center, and New Hanover Regional Medical Center.

But New Hanover County Sheriff’s Sergeant Jerry Brewer acknowledges there are still blind spots.

“In reality, could you put in an application for a pistol permit purchase or a carry conceal and have mental records in another state and us never be able to discover those? Yes, it’s true,” explained Brewer.


251. E.g., Chris W. Cox, You Can’t Afford To Sit Out This Fight, NRA (Dec. 31, 2013), http://home.nra.org/events/document/you-cant-afford-to-sit-out-this-fight (“The fact is, expanded background checks wouldn’t have prevented the tragedies we’ve seen committed by madmen. Nor will they deter criminals from committing the violence that occurs in our cities every day.”).
While the NICS system has some information on involuntary commitments, there is [no] federal law requiring states to submit that data. North Carolina law requires clerks of court here to enter all involuntary commitment information into the national database, but that’s not the case everywhere.

Moreover, beyond involuntary commitment information, there is no national database with comprehensive mental health records.252

Additional hybrids of public health and criminal justice databases also contemplate criminal enforcement of isolation and quarantine for mass contagion risks, such as the global Ebola viral outbreak in 2014,253 and even chronic health conditions such as obesity.254 As with all public records requests, the extent to which the government, pursuant to its police power, collects, collates, reviews, and publicly disseminates personal information in the interests of community health and safety requires a continual balance of interests as public policies and political priorities change over time.

As in every state, confidentiality provisions for medical information vary greatly in purpose and function. In North Carolina, where the near landmark LexisNexis255 case on public access to government databases was recently decided, the legally authorized mass collection of information may relate to significantly private matters, such as HIV testing and treatment.256 Public health information on persons with a communicable disease must be de-identified before reports subject to public records access are issued.257 Nevertheless, sometimes collected information will be public for some time before the legislature determines the balance of public and private interests requires a confidentiality exemption. In 2013, for example, North Carolina enacted for the purpose of forestalling a rash of identity thefts of discharged veterans a new


255. See supra Part III.A.1.


257. See, e.g., N.C. GEN. STAT. § 130A-143 (2014) (exempting from public record the mandated government collection of information on persons with AIDS or other disease required to be reported to the North Carolina Department of Public Health). See also Data Security and Confidentiality Guidelines for HIV, Viral Hepatitis, Sexually Transmitted Disease, and Tuberculosis Programs: Standards to Facilitate Sharing and Use of Surveillance Data for Public Health Action, CTRS. FOR DISEASE CONTROL & PREVENTION, http://www.cdc.gov/nchhstp/ProgramIntegration/docs/PCSIDataSecurityGuidelines.pdf (last visited May 11, 2015).
restriction on the release of records to the public of military service discharge documents.258

Despite the attempt to provide clear definitions and exceptions in public records law, overlapping federal and state confidentiality laws regarding medical information make determinations of what is excluded from public record disclosure particularly complex for custodians of records and members of the public alike. This is the case, notwithstanding the already difficult task of crafting a clearly defined public records request for a database and/or the metadata within it, as well as interpreting what constitutes compliance with the request.259 For example, in its privacy rule provisions, the Health Insurance Portability and Accountability Act (HIPAA)260 limits its scope of protected information to “individually identifiable health information,” in electronic, written or oral form,261 which includes the following:

[D]emographic information collected from an individual, that … is created or received by a health care provider, health plan, employer, or health care clearinghouse; and … relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present or future payment for the provision of health care to an individual, and … identifies the individual; or … with respect to which there is a reasonable basis to believe that the information can be used to identify the individual.262

Public records laws apply to broader formats of information, including “other documentary material, regardless of physical form or characteristic.”263 Therefore, HIPAA may not protect against public records requests for information in certain formats, such as metadata.

Even so, state law protections of medical privacy may create greater limits on public records access where broad federal laws such as HIPAA or the Family Educational Rights and Privacy Act (FERPA) would permit disclosure.264

258. N.C. GEN. STAT. § 47-113.2(a) (2014) (“All military discharge documents filed on or after January 1, 2004, shall be considered a public record, but for confidential safekeeping and restricted access to such documents, these documents will be filed with the registers of deeds in this State. These documents are exempt from public inspection and access except as allowed in subsections (b) and (m) of this section.”).

259. See supra notes 33-36 and accompanying text.

260. 45 C.F.R. § 164.504(g)(1) (2014) (applying HIPAA as follows: “A covered entity that performs multiple covered functions that would make the entity any combination of a health plan, a covered health care provider, and a health care clearinghouse, must comply with the standards, requirements and implementation specifications of this subpart, as applicable to the health plan, health care provider or health care clearinghouse covered functions performed”).


263. N.C. GEN. STAT. § 132-1(a) (2014); see supra Part II.B.

264. See, e.g., Nancy E. Tribbensee & Steven J. McDonald, FERPA and Campus Safety, NACUANOTES, Aug. 6, 2007, available at http://counsel.cua.edu/FERPA/publications/NACUANOTE.cfm (noting that FERPA, 20 U.S.C. § 1232g, permits selective emergency disclosures of otherwise protected student health or safety information, such as
Custodians of record, therefore, face serious challenges in ascertaining how the overlap of federal and state confidentiality laws apply to public records requests involving sensitive health information. Therefore, when public records requests for large government databases involve information that may include private medical information, it is vital that the agency understand what is deemed private and under which specific legal or policy provision(s), as well as whether there are exceptions to the exceptions.

2. Emerging Public Health Surveillance Databases

Often mass collection relates to collection of information on individuals over whom the government already has a supervisory role, such as inmates, public school students, and foster children. For example, public education records, including those involved with student health care, are increasingly database reliant, yet highly complex for custodians of record in the face of public records requests. Under FERPA, the educational institution may not disclose a student’s educational record, including records of immunizations, health testing, and school nurse or counseling visits, without the written consent of the parent or eligible student. At postsecondary institutions, however, medical and psychological treatment records of students are not defined as education records under FERPA, but are instead private treatment records subject to HIPAA for students who are in most cases eighteen years of age and older. The custodian of educational records, when addressing a public records request for an entire database of student public health information, would also have to consider information relating to contagious disease or suicidal thoughts, but not to “broadcast” disclosures to the public at large.


266. See Statewide Longitudinal Data Systems Grant Program, NAT’L CTR. FOR EDUC. STATISTICS, https://nces.ed.gov/programs/slds/ (last visited May 11, 2015) (working under a Federal grant, the North Carolina Department of Education has been taking part in the national Statewide Longitudinal Data Systems to track student success and learning over a number of years).


268. See 20 U.S.C. § 1232g (2014); 34 C.F.R. Subpart A § 99.1-.8 (2014) (addressing the privacy of students’ education records). FERPA protects the privacy of student education records, and applies to educational institutions receiving funds from the U.S. Department of Education. Therefore, private, religious, and home schools are not subject to FERPA privacy rules. See id.


270. 34 C.F.R. § 99.3 (2014).
whether contracted public health personnel work on school grounds, which may mean that both HIPAA and FERPA apply.\textsuperscript{271}

Government agencies may seek to share medical information with schools to ensure proper health services are provided.\textsuperscript{272} While this would significantly expand disclosure of personal student information between state agencies, privacy protections would likely continue to create exceptions to public records access. In contrast, in emergencies, such as when students make a credible threat to harm themselves or others, both HIPAA and FERPA contain exceptions permitting disclosures to parents and law enforcement.\textsuperscript{273} In such cases, the student’s private educational and medical records are held by yet another government agency (i.e., law enforcement) and may eventually be maintained as records within the court system, which in turn may evade the previously noted exceptions to public records access. Note that according to the Centers for Disease Control, the third most common cause of death among adolescents in the United States is suicide; thus, many students are subjected to potentially greater privacy intrusions when school records include mental health records.\textsuperscript{274}

Such information has the potential to transform in character from private to public, to even be mandated for collection, or to a new use with different overlapping state and federal laws. For example, mandated government collection and public record information on school violence has now begun to focus on information from medical and mental health treatment providers in order to disclose incidence rates of violence to the public at large. This information is not always easily de-identified, such as:

- Jeanne Clery Act and Violence Against Women Act – federal laws requiring disclosure of crime statistics to the federal government and to the public on college campuses\textsuperscript{275}
- Campus SaVe Act of 2012 – increasing school and campus transparency of sexual violence incidents\textsuperscript{276}

\textsuperscript{271} Joint Guidance, supra note 258.
\textsuperscript{272} Michael S. Lancaster, Release of Information to Schools (2006) (permitting and encouraging North Carolina Local Management Entities (LMEs), coordinating public health systems, to release personal medical information to local school districts). Note that once the LMEs provided this information to the schools, however, the memorandum does not clarify that the records may now fall within different FERPA protections if a public records request for such information were made to the school directly. See id.
\textsuperscript{273} See 45 C.F.R. § 164.512(j) (2014) (HIPAA exception for serious threats); 45 C.F.R. § 164.502 (2014) (HIPAA exception for disclosure to parents of minors); 34 C.F.R. §§ 99.31(a)(10), 99.36 (2014) (FERPA exception for emergency disclosure to appropriate parties); 45 C.F.R. § 164.512(c) (2014) (HIPAA permitted disclosures about victims of abuse, neglect and domestic violence).
\textsuperscript{276} Id.
Comprehensive School Safety Initiatives - The National Institute of Justice research funding for involving data collection and dissemination.\footnote{In 2014, the National Institute of Justice (NIJ) made available approximately $15 million for multiple grants to fund research to examine the root causes of school violence and to develop new technologies, apply evidence-based practices, and test pilot programs to enhance school safety. See \textit{Comprehensive School Safety Initiative: Dear Colleague Letter}, NAT'L INST. OF JUSTICE (April 11, 2014), http://nij.gov/funding/Pages/fy14-dear-colleague-school-safety.aspx.}

Again, the influence of criminal justice on public health, with its tendency towards disclosure of individual information as a matter of public record, is readily apparent.

Under its police power, the state has the authority to regulate public health and medical care for the protection of its citizens and residents, which allows for regulation of health care professions, often in large government databases.\footnote{This is a longstanding proposition supporting state public health intervention and policy. See \textit{Nat'l Fed'n of Indep. Bus. v. Sebelius}, 132 S. Ct. 2566, 2678 (2012) (noting the police power of each of the fifty states, separate from federal authority, in consideration of the scope of the individual mandate in the Affordable Care Act); \textit{see also} Feldman v. City of Cincinnati, 20 F. Supp. 531, 541 (S.D. Ohio 1937) (quoting Wilson v. Zanesville, 130 Ohio St. 286, 297-98 (Ohio 1935)) (“Where new evils detrimental to public health, morals, and safety spring up due to the march of civilization, the evils must be met by proper police regulations, and such regulations are of necessity within the police power.”); \textit{see also} Matter of DeLancy, 67 N.C. App. 647, 654 (N.C. Ct. App. 1984) (upholding the regulatory authority of the North Carolina Board of Dental Examiners under its police power over “public health and welfare”).} Choosing which areas of public health to regulate is always a compelling question for the state, and one that involves changing social attitudes as well as medical trends.\footnote{For example, in 2011, Montana’s strict regulation of medical marijuana, including restrictions on providers and registered patient cardholders, was upheld by the Montana Supreme Court pursuant to its police power. Mont. Cannabis Indus. Assoc. v. State, 286 P.3d 1161 (Mont. 2012); \textit{see also} Thomas J. Bourguignon, Note, \textit{Montana Cannabis Industry Association v. State of Montana and the Constitutionality of Medical Marijuana}, 75 MONT. L. REV. 167, 170 (2014); \textit{see also} Greg Botelho, \textit{Alaska Becomes Latest State to Legalize Marijuana Use}, CNN (Feb. 25, 2015, 1:24 AM), http://www.cnn.com/2015/02/24/us/alaska-marijuana/} Public health regulation necessitates government agency documentation of certain forms of individual medical care, which again invokes consideration of whether any of those records become public records. If so, what would result from a public records request for an entire database of public health records?

In addition to the changing views of privacy needs addressed by legislative bodies, clerks and courts struggle with discretionary compliance decisions involving important competing public and private interests. These interests, for example, are inherently difficult to determine in matters of public health affecting larger or more vulnerable populations. For the requestor of information, that the ease of release of electronic information is technologically available at the touch of a button must increase the frustration when access is denied.

In \textit{State Department of Public Health v. Superior Court}, a split decision now pending before the California Supreme Court, the California Court of Appeals
granted an investigative news organization public records access to ordinarily private health information.\textsuperscript{280} It specifically permitted disclosure of information on patient care violations in a facility housing persons with mental illness and developmental disability, but not to personally identifiable information or information including a patient’s medical conditions, history of mental disability, or the risk the violation presented to the patient.\textsuperscript{281} De-identification, however, is not always a reasonable compromise, particularly with regard to newly emerging concerns involving high profile patients few in number, as seen in the current Ebola crisis.\textsuperscript{282}

When the information is mandated for collection, however, the appearance of confidentiality even for patient medical records begins to appear less confidential than it was. The “interests of the herd” in basic public health policy have historically warranted valuing public interests in disclosure over individual privacy.\textsuperscript{283} According to the Centers for Disease Control (CDC), environmental public health surveillance can be used to:\textsuperscript{284}

- Quantify the magnitude of a public health problem
- Detect unusual trends in health, exposures, and hazards
- Identify populations at risk of environmentally related diseases or of exposure to hazards
- Generate hypotheses about the relationship between health and the environment
- Direct and evaluate control and prevention measures and individual actions
- Facilitate policy development

The large and varied public health data sets created by the CDC contain complex surveillance and survey data sets within large databases, but they are now using metadata applications to re-catalog them and re-assess the information

\textsuperscript{281} Id.
\textsuperscript{282} See supra Section II.
\textsuperscript{283} See, e.g., Mary Holland & Chase E. Zachary, \textit{Herd Immunity and Compulsory Childhood Vaccination: Does the Theory Justify the Law?}, 93 Ore. L. Rev. 1, 4 (2014) (“[H]erd immunity is the central rationale for compulsory vaccination, and the U.S. Supreme Court has long upheld the right of states to mandate vaccines under certain circumstances.”).
\textsuperscript{284} \textit{Indicators and Data}, CTRS. FOR DISEASE CONTROL & PREVENTION, http://ephtracking.cdc.gov/showIndicatorsData.action (last visited May 11, 2015); see also Sudden Unexpected Death Data Enhancement and Awareness Act, Pub L. No. 113-236, 128 Stat. 2831 (requiring an increase in public health electronic surveillance data targeted at demographic, cause of death, and clinical history information for still birth and sudden unexplained death of infants and children across the United States).
they contain as a grouped set. The original purpose for research naturally changes over time, particularly when access changes, but one must question whether the patient’s consent for the research is renewed, or whether the government even asks. As stated by the researchers, proud of their new uses for the information, the metadata was initially put in place for internal CDC purposes, but they are now “exploring methods for wider applicability.” And yet, the CDC has acknowledged that its own data security for large-scale surveillance and data sharing across the agency’s many divisions is inconsistent: “Maintaining confidentiality and security of public health data is a priority across all public health programs. However, policies vary and although disease-specific standards exist for CDC-funded HIV programs, similarly comprehensive CDC standards are lacking for viral hepatitis, STD, and TB prevention programs.”

Federally mandated personal health information collection may be subject to Freedom of Information Act provisions, not wholly exempt from public access. In U.S. Department of State v. Ray, the United States Supreme Court determined that a Florida attorney’s public records request relating to deported Haitians could not include personally identifiable information, as it fell within the public records exception for medical, personnel and similar records. Although the lower courts had determined that there was a de minimus risk of privacy invasion by providing the names and addresses of those deported, the Supreme Court disagreed because the detainees had been promised confidentiality before they agreed to be interviewed. The state also asserted that the detainees could experience community shame from disclosing their cooperation with the government, as well as the risk of linking their identity to other personal information already disclosed in the un-redacted portions. The question was not whether there was an invasion of privacy, but whether there was a “clearly unwarranted” invasion of privacy.

To determine whether a request for records is unwarranted requires a familiar balancing of the interests between personal privacy and government transparency; a test that may be highly individualized. More recent federal court

286. Id.; see also Iowa Tracking Program, IOWA DEP’T OF PUB. HEALTH, http://www.idph.state.ia.us/EHS/EPHT.aspx?pg=EPHTMetadata (last visited May 11, 105) (a state example of environment public health tracking).
289. Id. at 170.
290. Id. at 177.
291. Id. at 166 (relying on 5 U.S.C. § 552(b)(6) (2014)).
decisions have assumed a substantive due process right to informational privacy exists, including implementation of such a balancing test. Thus, the interest of the attorney requesting the information, on behalf of his clients, was also taken into account: that is, “the public interest in learning ‘whether our government is honest to the public about Haiti’s treatment of returnees.’” The Court also weighed the potential benefit to the public of disclosure or Reverse Sunshine, in this case the benefit to the public of naming names, and ultimately found such benefit to be minimal. Had the request applied to an entire database of information, applying such a nuanced balancing test would be substantially more challenging, with the risk of unwarranted disclosure and error in compliance even greater.

V. A NEED FOR A MORE ROBUST PRIVATE RIGHT OF ACTION TO PROTECT INDIVIDUAL PRIVACY FROM UNWARRANTED PUBLIC RECORDS DISCLOSURE

Due to notoriously limited remedies and access to those remedies for individuals whose information is unduly disclosed as a matter of public record, it bears consideration why better remedies are needed. Despite a history of jurisprudence recognizing a right to privacy, albeit under competing theories, providing remedies for a governmental infringement on personal privacy has been a longstanding concern. As Samuel Warren and Louis Brandeis stated in 1890 regarding informational privacy:

> Recent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the, individual what Judge Cooley calls the right “to be let

---

292. See Warner v. Twp. of S. Harrison, 885 F. Supp. 2d 725, 739 (D.N.J. 2012) (applying the balancing test articulated in Fraternal Order of Police and relied upon by the United States Supreme Court majority in NASA when weighing competing individual privacy and governmental disclosure interests).

293. Ray, 502 U.S. at 172.

294. Id. at 176.

295. See, e.g., Charles N. Davis, Milagros Rivera-Sanchez, & Bill F. Chamberlin, Sunshine Laws and Judicial Discretion: A Proposal for Reform of State Sunshine Law Enforcement Provisions, 28 URB. LAW. 41 (1996) (criticizing overreliance on judicial discretion in enforcement of open meetings laws); Angela Dougherty, Professional License Applications Subject to Public Disclosure?, 26 WYO. LAW. 20 (2003) (expressing identity theft concerns with licensing boards publicly sharing personal information on members of the profession); Id. at 21 (“[R]edaction of personal identifiable information may be a feasible, albeit burdensome, alternative [to denial of records] for the custodian in complying with public records requests absent a specific statutory exemption.”).

296. See Reva B. Siegel, How Conflict Entrenched the Right to Privacy, 124 YALE L.J. FORUM 316 (2015) (interpreting the legacy of Griswold as the origin of a judicial recognition of a constitutionally supported moral right to privacy); Samuel C. Rickless, The Right to Privacy Unveiled, 44 SAN DIEGO L. REV. 773 (2007) (categorizing the moral right to privacy as universal, but the legal right to privacy as limited to tort protections against an intrusion upon seclusion or a constitutional 4th Amendment right); but see Sonu Bedi, Repudiating Morals Legislation: Rendering the Constitutional Right to Privacy Obsolete, 53 CLEV. ST. L. REV. 447 (2005-2006).
alone.” Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that “what is whispered in the closet shall be proclaimed from the house-tops.” For years there has been a feeling that the law must afford some remedy for the unauthorized circulation of portraits of private persons; . . . .

With the advent of public records requests for entire databases and their accompanying metadata, these concerns are all the more relevant today.

A. Limited Remedies for Government Non-Compliance

In a Digital Age, the reasons a government agency may deny a public records request vary. For example, state and federal jurisdictions coping with public records requests for an increasingly greater amount of government information have attempted to rely on existing restrictions on requests for voluminous records. However, because this may too easily limit public access, since 1997 when a federal government agency denies a public records request in whole or in part, the agency must now “make a reasonable effort to estimate the volume” of what is withheld and “provide any such estimate to the person making the request.” That is not the case with every state jurisdiction, where denials may or may not require a detailed explanation.

In general, if a requestor wishes to assert that an agency is noncompliant in violation of a Public Records Act, recognition of and access to effective remedies is notably difficult. Typically, remedies include injunctive or declaratory relief, with a risk of being held liable for the court costs of the opposing party.

---

297. Samuel D. Warren & Louis D. Brandeis, The Right to Privacy, 4 HARV. L. REV. 193, 195 (1890) (emphasis added) (addressing interference with personal privacy by the press and its use of improved photography and technology, as well as the remedies of claims of libel and slander).
298. See supra Section III.B.
300. See, e.g., MD. CODE REGS. 10.01.08.03 (2014) (emphasis added) (redefining in more detail how requests for records are to be handled by the Maryland Department of Health and Mental Hygiene, and providing substantial discretion to State government in explaining the reason for denial). The text of the regulation follows:
   COMAR 10.01.08.03 Procedures Regarding Inspection or Copying of a Record.
   A.—B. (text unchanged)
   C. Response to Requests.
      (1) The custodian shall respond to a record request as soon as possible, but not later than 10 business days after the receipt of the request, by:
         (a) Providing access to the requested records;
         (b) Denying access to the record or parts of the record with an explanation for the denial;
   Rule T1, 247.
301. See, e.g., 5 ILL. COMP. STAT. 140/11 (2014); see also Cline v. Hoke, 766 S.E.2d 861, 863 (N.C. Ct. App. 2014) (addressing how to define the proper custodian when “In order to compel an unresponsive custodian to fulfill this statutory duty, a party must sue the custodian of those records in the custodian’s official capacity”); Francis v. Wash. State Dep’t of Corr., 313 P.3d 457 (Wash. Ct. App. 2013) (holding that an inmate was entitled to court costs and the penalty fees of $4,495 for
However, litigation is a long, expensive, and unpredictable process, and those without substantial means or resources cannot easily enforce their rights to either obtain public records or protect themselves against public records access. As stated by the Washington Court of Appeals in 2013, when justifying a reasonableness rather than intentional standard for bad faith noncompliance: “Were we to accept the Department[] of Correction’s] interpretation, agencies could safely respond to record requests from incarcerated persons with cursory or superficial searches, knowing that inmates would find it difficult to determine whether records were overlooked and all but impossible to produce admissible evidence of wrongful intent.”

Consider the 2013 opinion by the federal District Court of the District of Columbia in Citizens for a Responsibility and Ethics in Washington v. U.S. S.E.C., in which the court confessed to its weak role in policing the Security and Exchange Commission’s destruction of its own records, ensuring they are no longer available through public records requests. Here, an agency key to the public trust is permitted to essentially police itself. The court’s rationalization in providing no remedy for the complainants is startling:

“Rather, the record suggests an agency aware of the potential enormity of the task at hand, but attempting to clarify the scope of the problem, making some efforts to retrieve documents that might still exist, identifying additional sources of information regarding the relevant documents, and counseling employees regarding future document preservation.”

In short, the court makes clear that the statutory mandate governing deliberate destruction of records in this case only allows for either internal policy reform by the agency or legislative action by Congress, not individual legal action unless the claimant proves the difficult standard of “clear error of judgment”.

Also, the burden of proof for a FOIA violation may be challenging for individuals seeking to deter release of information. For example, in New York in Mulgrew v. Board of Education, the government’s choice to disclose public records must be “arbitrary and capricious” and an “unwarranted invasion of personal privacy” to be considered a state violation of the Freedom of

302. See, e.g., Jackson v. Charlotte Mecklenburg Hosp. Auth., 768 S.E.2d 23, 24 (N.C. Ct. App. 2014) (regarding application of the legal settlement exception to the public records act, in which it took a year to trial, and another year and a half to appeal an issue that related to a straight-forward matter of basic statutory interpretation and plain language).
303. Francis, 313 P.3d at 467.
305. Id. at 150.
Information Law. In justifying its decision not to grant the teacher’s union petition to force the New York City Department of Education to redact identifiable information on Teacher Data Reports requested by media groups, information which included teachers’ names and individual performance rankings, the Court listed numerous examples of other state court decisions protecting governmental discretionary decision making to release personal information. The release in Mulgrew was met with “anguish” by thousands of teachers who had been told by their administration that the ratings would be confidential. As with all large data sets produced as public record, it was easily disseminated once the decision was made to release the information: “The data was handed to the news media on CDs, which contain spreadsheets listing teachers’ scores for the 2007-08, 2008-09 and 2009-10 school years. Roughly 12,000 teachers were given teacher data reports each year.”

For the government, one of the more complex challenges of maintaining hybrid public/private records, difficult to redact, is that sanctions for noncompliance may exist in both Public Records Act provisions and in statutory confidentiality provisions. For example, differing records preservation laws or policies may apply. A government hospital may have its own records retention policies pursuant to state and federal law, but if any records are defined as public records, then a public records law may prohibit destruction subject to criminal penalties. With respect to HIPAA protected information, unduly disclosing large data sets can be financially precarious. In March 2014, Skagit County, Washington, agreed to settle potential HIPAA violations affecting more than 1,500 public health department patients with a $215,000 monetary settlement. According to the news report:

OCR [Office of Civil Rights] opened an investigation of Skagit County upon receiving a breach report that money receipts with electronic protected health information (ePHI) of seven individuals were accessed

---

308. Id. at 790.
309. See Fernanda Santos, City Teacher Data Reports Are Released, SCHOOLBOOK, WNYC (Feb. 24, 2012, 11:21AM), http://www.wnyc.org/story/301783-teacher-data-reports-are-released/ (“After a long legal battle and amid much anguish by teachers and other educators, the New York City Education Department released individual performance rankings of 18,000 public school teachers on Friday, while admonishing the news media not to use the scores to label or pillory teachers.”).
310. Note that additional remedies not discussed in this article include expungement rules and process.
311. See N.C. GEN. STAT. § 132-3(a) (2014) (“Prohibition—No public official may destroy, sell, loan, or otherwise dispose of any public record, except in accordance with G.S. 121-5 and G.S. 130A-99, without the consent of the Department of Cultural Resources. Whoever unlawfully removes a public record from the office where it is usually kept, or alters, defaces, mutilates or destroys it shall be guilty of a Class 3 misdemeanor and upon conviction only fined not less than ten dollars ($10.00) nor more than five hundred dollars ($500.00).”).
by unknown parties after the ePHI had been inadvertently moved to a publicly accessible server maintained by the County. … Many of the accessible files involved sensitive information, including protected health information concerning the testing and treatment of infectious diseases. OCR’s investigation further uncovered general and widespread non-compliance by Skagit County with the HIPAA Privacy, Security, and Breach Notification Rules. 313

Despite the various privacy laws restricting access to personal information, keep in mind when such information reaches the courts, another opportunity for public disclosure arises. Most records of judicial proceedings, including court transcripts, and the evidence presented are matters of public record with their proceedings falling squarely within the definition of open meetings. 314 The time and place of proceedings, and some of the dispositional information, such as bond amounts and sentencing, are provided to the public as matters of public record in easily accessible online databases. 315 Thus, at least with respect to the criminal justice and public health systems, the tendency towards public disclosure of personal information in public databases and registries comes full circle again. 316

More commonly, litigants are allowed to invoke qualified privileges of communication to exclude evidence of confidential medical records, or to prevail on the court to admit them in the interests of justice. 317 Even when matters are otherwise protected by statutory or common law qualified privilege or other law of confidentiality, a judge may have discretion to reveal information admitted as evidence in the interests of justice. 318 Judges also have the discretion to seal and then unseal court records. 319 As stated by the North Carolina Court of Appeals in

313. Id. (emphasis added).
314. See generally N.C. Const. art. I, § 18 (detailing qualified right of access to court records); N.C. GEN. STAT. § 7A-109(a) (2014) (detailing courts’ record keeping procedures); but see Virmani v. Presbyterian Health Servs. Corp., 515 S.E.2d 675, 685 (N.C. 1999) (permitting judicial denial of access to court records in the interests of the fair administration of justice or as a matter of public policy when openness is “more harmful than beneficial”).
315. See generally N.C. GEN. STAT. § 143-318.10 (2014) (defining open meetings).
316. See infra Appendix A, How to Find Public Information About People Online.
318. This article will not focus significantly on evidentiary privileges of information, although the subject of their scope in a digital age when there is a purported reduced reasonable expectation of privacy is an important parallel topic.
319. See N.C. GEN. STAT. § 8-53 (2014) (permitting judge to compel disclosure, despite physician-patient privilege, “if in his opinion disclosure is necessary to a proper administration of justice”). However, statutory directives may wholly limit judicial discretion to disclose matters into the public record. For example, North Carolina law now strictly limits public disclosure in judicial proceedings of the identity of a woman who has obtained an abortion, unless she specifically consents to disclosure. See N.C. GEN. STAT. § 90-21.123 (2014).
2011 in *France v. France*, only a year before the same court’s decision in *LexisNexis*, to permit a public records request for an electronic copy of an entire database: “[c]ertain kinds of evidence [in court] may be such that the public policy factors in favor of confidentiality outweigh the public policy factors supporting free access of the public to public records and proceedings.”

Ultimately, even with a potential recognition of an informational right to privacy, or a more generous standard of liability, additional federal penalties for particularly sensitive categories of records, few individuals will realistically be able to enforce their privacy rights in the face of Public Records Acts goals of transparency. Even fewer will be able to safely monitor their privacy rights when their information is disseminated and re-disseminated to third parties, including large commercial interests and criminal offenders. Journalists emphasize litigation to enforce public access to government information under Sunshine Laws, but they have traditionally been interested only in expanding access and have the financial means to enforce such access. They are unlikely to have standing to file civil claims or to wish to serve as the “fourth estate” to restrict access and prevent unwarranted disclosure of the personal information of individual citizens. Thus, when remedies are weak or inaccessible for public records violations involving unwarranted disclosure of personal information, the oft quoted tenet of Justice Brandeis that “sunlight is said to be the best of disinfectants” against government corruption is illusory.

**B. Inaccuracy, Misrepresentation, and Compromised Security in the Digital Wild Frontier**

In an ideal world, large government databases as public record would be well managed, well resourced, secure from cyberattack, and assiduously monitored for ethical compliance. However, this has not been the case for big data made public, whether produced by the government, or produced commercially.

---

321. 705 S.E.2d 399, 407 (N.C. Ct. App. 2011) (internal citation omitted).
322. See sources cited supra note 7.
324. See N.C. GEN. STAT. § 132-3(a) (2014).
326. See *Louis D. Brandeis, Other People’s Money* (1913) (originally collected in a series of installments by Harper’s Magazine), available at http://louisville.edu/law/library/special-collections/the-louis-d.-brandeis-collection/other-peoples-money-chapter-v (“Publicity is justly commended as a remedy for social and industrial diseases. Sunlight is said to be the best of disinfectants; electric light the most efficient policeman. And publicity has already played an important part in the struggle against the Money Trust.”).
The risk of cyberattack on large databases by unauthorized criminal and terrorist elements is a matter of longstanding concern, which is exacerbated by increasing technological sophistication currently matched by increasing reliance on digital storage of highly sensitive information. In 2015, Estonia, the nation that invented Skype and leads technology innovation in the European Union, initiated a project to create digital embassies:

The project plans to use cloud technology and off-site servers to ensure all Estonian registries - from public records such as property ownership to secure ones like population records - will be duplicated and stored internationally, with an instantaneous, entirely virtualized, back-up process. Born of advancing technology several years ago but bogged down by bureaucracy, the concept was recently renewed by fear.

On a more innocuous level, inadvertent misrepresentation of the information collected may also put the security of the information at risk and compromise informational privacy. For example, the information collected by the government may be partially exempt from public disclosure, and that fact may not be disclosed on the public database and registry websites, creating the impression that the public record is complete. Some of the information may be less accurate, particularly when large databases are difficult to monitor and update in a timely manner; that is, less accurate than if a public records request were made directly to the agency. The practicalities of working with government bureaucracies, and agencies that may be understaffed or under-resourced places added strain on the person seeking to obtain his or her own records.

For example, the North Carolina Department of Health and Human Services (DHHS) indicates that early vital records may be kept on microfilm, while later


330. Molly McCluskey, Estonia Redefines National Security in a Digital Age, ALJAZEERA (March 20, 2015), http://www.aljazeera.com/indepth/features/2015/03/estonia-redefines-national-security-digital-age-150318065430514.html (highlighting the renewed cyberattacks from Russia against the EU and Estonia). Note that Articles 22 and 25 of the Vienna Convention protect diplomatic properties and communications, but do not currently include off-site data centers serving embassies and their databases of national security information. Id.

331. For example, the author’s salary information and title have been significantly inaccurate on public employee salary databases.
versions are more easily available online. Currently, there is a backlog of requests for official certificates of records, which can cause delays:

“Due to request volume, processing time for standard orders for birth certificates from 1971 to present may take up to five weeks. Standard orders for other types of certificates may take six to eight weeks. Requests that are accompanied by an expedite fee are usually processed within three to five business days from the time N.C. Vital Records receives the request.”

Despite the obviously sensitive nature of some information contained in public databases, most online databases acknowledge a risk of inaccuracy, but do not discuss what information was not disclosed through exemption or otherwise. The possibility for misrepresentation could be dire in certain circumstances. For example, the National Sex Offender Registry website first points out that it is an “unprecedented public safety resource,” drawing together numerous state, local and tribal databases into one search site. However, at the bottom of the page, its last line discloses: “The search criteria available for searches are limited to what each individual Jurisdiction may provide. Search results should be verified by visiting the providing Jurisdiction’s Public Registry Website for further information and/or guidance.”

If a public citizen relied on this database, assuming that a neighbor or co-worker was or was not a registered sex offender, and that information was incorrect, the potential consequences could be very serious indeed. As has been noted since 2001 by the Library of Congress:

Even among agencies that house records solely for the purpose of public access, such as public libraries, there is recognition that cataloguing and search functions are extremely difficult to maintain accuracy and efficiency because of the voluminous data. “Searching is similar to automated cataloging in that neither can overcome the absence of data inferable from a resource, and Web resources will not evolve stable self-describing mechanisms for a long time, if ever; such mechanisms are not yet even being broadly discussed. Desired characteristics such as creation date, revision date, and expiration date, just are not easily available from most Web resources. Inappropriate titling, weak or absent content descriptors - we can go on and on. The absence of these descriptors, or their presence in corrupt or unrecognizable form, within a Web resource corrupts the results of any

335. Id.
searching; and we can expect such problems to grow for a long time rather than abate.”336

A related concern exists in public records citing to website links that eventually disappear over time, preventing continued monitoring of accuracy.337

Beyond the concern regarding inaccuracy in government databases is one of misuse and fraud. For example, patients in most cases will have greater access to their own personal information under various federal and state laws than they would to the public information of others.338 It is essential that patients, in particular, have such access to understand their personal health needs, and to correct any inaccuracies that may influence future care or health insurance. Nevertheless, notes and incomplete drafts of records may still be inaccessible to the patient, for while HIPAA has been linked to a trend in increasing patient access to records,339 psychotherapy notes are expressly excluded.340

In addition, medical identity theft concerns reportedly increased twenty-two percent in the last year,341 according to the Federal Trade Commission (FTC), and the patient’s ability to monitor his or her own medical record has become crucial.342 The patient’s medical information is now disclosed to the thief and
anyone he or she wishes to share it with (or sell it to).\footnote{See, e.g., Laura A. Feldman, Note, \textit{Determining the Proper Standard of Causation to Support a Conviction under 18 U.S.C. § 1347 When Healthcare Fraud ‘Results in Death’}, 98 Iowa L. Rev. 2061, 2064 (2013) (addressing the risk of denial of insurance coverage, unexpected bills, and denial of care due to medical identity theft).} Medical fraud also creates a very serious health risk, because if medical records are intertwined with that of the perpetrator, then in an emergency one may be given unneeded and potentially dangerous medications and procedures.\footnote{See id.} According to the FTC, there have also been instances noted in the media of hospital personnel selling thousands of patient identities; thus, it is not always a matter of a lost or stolen wallet, but may be an internal corruption problem.\footnote{See id.} The FTC and consumer advocates recommend that patients regularly obtain a copy of their medical records to ensure that they are accurate and that no medical identity theft has occurred.\footnote{See Fed. Trade Comm., supra note 331.} But this is all the more reason to ensure that individual health information is not generally accessible in government databases as a matter of public record.

Foster children\footnote{Seth Freed Wessler, \textit{Preying on the Vulnerable: Foster Youth Face High Risk of Identity Theft}, NBC News (July 21, 2014, 4:11AM), http://www.nbcnews.com/feature/in-plain-sight/preying-vulnerable-foster-youth-face-high-risk-identity-theft-n157641.} and military personnel\footnote{Erica Sandberg, \textit{Military Families Remain Easy Prey for ID Theft}, Fox Business (March 5, 2014), http://www.foxbusiness.com/personal-finance/2014/02/14/military-families-remain-easy-prey-for-id-theft/.} should also be aware of an increased risk of identity theft, because of their transience and the voluminous paperwork often associated with these populations, factors not always within the patients’ ability to monitor. These are populations already subject to government supervision and more likely to have personal information, such as social security numbers and dates of birth, subsumed into large government databases as a result.

Judges may demonstrate more trust in government efficiency and electronic records management than the technology industry itself. For example, in 2008, the Kentucky Supreme Court in \textit{Commonwealth v. Chestnut} held that problems in responding to a voluminous request for an inmate’s entire record, requiring careful redaction, did not outweigh the need for the information, despite the fact that it was clearly “tedious and time-consuming work” to respond.\footnote{250 S.W.3d 655, 664 (Ky. 2008).} The Court held that “[a]ny relief here must come from the General Assembly in the form of restricting access to public records, extending the time period for state agencies to respond to open records requests, or providing necessary additional funds to allow state agencies to comply timely and fully with open records requests.”\footnote{Id.} Alternatively, the court suggested that the Department of Corrections improve its
filing organization internally for greater efficiency and cost management.\textsuperscript{351} Of interest here, however, was the court’s final point:

But we reject the DOC’s argument that a possible inadvertent disclosure of any such protected matter is a reason to deny open records requests such as Chestnut’s. \textit{We trust that the DOC will scrupulously perform its duty} to ensure that any privileged materials are not provided to inmates, or to anyone else, under an open records request. But it is clear to us that the prospect of a public agency’s potentially negligent disclosure of protected items is simply an insufficient reason to thwart the openness the General Assembly sought to achieve when it enacted the Open Records Act.\textsuperscript{352}

The agencies themselves do not carry the same level of trust in their performance. Government agency websites providing public records information often include a prominent disclaimer related to the risk of inaccurate information. For example, the North Carolina Department of Health and Human Services (DHHS) website noted above providing vital records, states in its disclaimer:

“All information provided in this web site is believed to be accurate and reliable; however, the N.C. Department of Health and Human Services (DHHS) assumes no responsibility for the use of this information. . . . If you believe that information obtained from the N.C. DHHS web site is inaccurate or out-of-date, please notify the N.C. DHHS webmaster.”\textsuperscript{353}

Increasingly, critics have become concerned that management of these data systems cannot be adequately controlled, particularly when the government must use private companies to create and monitor software. For example, with regard to the North Carolina Department of Education Statewide Longitudinal Data Systems, one watchdog group warns:

“No matter how much the State Board of Education tells us our personal information is protected, they can’t explain away the fact that private data collecting companies need access to the details of our children in order to inform authorities how to control factors to get the students ‘college and career ready.’”\textsuperscript{354}

Nevertheless, the dissent in one of the few opinions directly addressing public records requests for whole databases, that of Justice Huffman of the

\textsuperscript{351} See id. at 665.
\textsuperscript{352} Id. at 666 (emphasis added).
\textsuperscript{353} N.C. DEP’T HEALTH & HUMAN SERVS., supra note 322.
\textsuperscript{354} Ann Kone, \textit{What is Statewide Longitudinal Data System?}, WATCHDOGWIRE (Sept. 25, 2013), http://watchdogwire.com/northcarolina/2013/09/25/what-is-statewide-longitudinal-data-system/ (“The compilation of very private student information underpins the trajectory of our present government to push states away from local control of schools to a nationalized system of education. Nationalization requires equalization, and in the world of equalization, data is king.”).
California Court of Appeals in *Coronado Police Officer’s Association v. Carroll*, aptly warned of another risk in using personal privacy for mass collection of information -- to mask government misconduct:

Privacy from governmental snooping into the private or even public affairs of citizens is provided by a comprehensive scheme of public inspection of the government’s records under the Act, except where there is a legitimate need to permit governmental secrecy. (§ 6253) The public defender’s office is a governmental agency, and no matter how lofty its stated purposes, it is still not entitled to collect intelligence files on citizens without some form of protection for the privacy rights of those citizens.\(^\text{355}\)

Such a “lofty goal” by the court to protect the individual from government corruption, however, does little to address the reality of inept maintenance and unwarranted disclosure of the government’s collection of information on individuals.

Blind trust by the courts in the Digital Age, or in truth the Digital Wild Frontier, does not necessarily bode well for the individual privacy interests at stake, with few practicable remedies available when violations occur.\(^\text{356}\) Eventually, complaints and litigation addressing Public Records Act violations due to unwarranted disclosure of personal information may impact judicial expectations of government competency in file management; this is especially likely if compliance with public records requests for databases and metadata do not properly redact confidential information. Before waiting on litigation remedies, however, it would be more prudent for public records custodians and managers to engage in practical means of better securing their information and communicating with the public how they do this.\(^\text{357}\)

VI. EMPOWERING THE PUBLIC IN A DIGITAL AGE TO ENSURE PROPER STEWARDSHIP OF THE BALANCE OF GOVERNMENT TRANSPARENCY AND INDIVIDUAL PRIVACY PROTECTIONS

Thus, as we fight to uphold the civil liberties we have been given, including the right to government transparency in the form of increasingly complex electronic public records, we must also be mindful of how far we are willing to go to invert the private to the public. Although it may be tempting to continue to expand the legal definition of public record to lengthen the list of format types,

\(^\text{355}\) 131 Cal. Rptr. 2d 553, 565 (Cal Ct. App. 2003) (denying a public records request for a database of offenders maintained by a county public defender’s office).

\(^\text{356}\) See supra Section VI.A.

\(^\text{357}\) See infra Section VI. Similar caveats are now being offered in the commercial world. “If we cannot organize the [digital information] system as a whole, then we will need to create our own small, secure-areas, and/or be more critical and circumspect in our business interactions.” Ors Penzes, *Information Security Challenges for Companies in the Digital Age*, 41 N. Ky. L. Rev. 471, 486 (2014).
such as video or metadata or the next new form, the all-inclusive key term in most public records statutory definitions is “documentary material, regardless of physical form or characteristics.” As technology evolves, most state law definitions of public record expand the list of accepted formats, but little else, without considering that the heart of the public records request is the information. In contrast, the Presidential Records Act and other federal statutes more specifically define what is and is not documentary material, as well as what is or is not a personal or private record of presidential staff. Within the scope of Sunshine Laws, private citizens deserve at least the same level of protection over their private information as that given to government officials. The spirit of the various Public Records Acts seeks to shine the light of transparency on whether the government is properly doing its job, not to shine a light on the private lives of its citizens without a sufficient connection to a government function. If mass collection of information on citizens is not relevant to direct justifiable government action, then the information should not be authorized for collection at all.

Thus, with respect to form and scope of permissible public records requests, the statutory definition of a public record may be simplified as follows to anticipate future technological advances:

“Public records” defined

(a) “Public record” or “public records” shall mean all documentary material, regardless of physical form or characteristics, made or received pursuant to law or ordinance in connection with the transaction of public business by any agency of [state] government or its subdivisions.

(b) Agency of [state] government or its subdivisions shall mean and include every public office, public officer or official (State or local, elected or appointed), institution, board, commission, bureau, council, department, authority or other unit of government of the State or of any county, unit, special district or other political subdivision of government.

(c) “Documentary material” shall mean recorded information which has a direct effect upon the carrying out of official government duties and activities, but does not include:

(1) recorded information otherwise protected by law from disclosure;

(2) personal information of government personnel or private individuals; or

(3) proprietary software created or received by the government for the sole purpose of informational storage and maintenance structures.

(d) “Personal information” shall mean all documentary material of a purely private or nonpublic character, which does not have a direct effect upon the carrying out of government business.

Note that database and metadata are not defined, but they could be, as seen in the 2014 Maryland amendments to its Public Records Act. Recall that metadata has multiple possible meanings and a state jurisdiction would need to decide which it preferred for a definition of public record format.

If the Presidential Records Act were to guide reform of a typical state public records law, the state would abandon access to records that only relate to government functions, but would instead permit public access to those records that have a direct effect on official duties and activities. While some may argue this would pull the shade on government transparency, it does no more than provide the protections that government officials have carved out for themselves under the glare of Sunshine Laws. Moreover, as seen in the Presidential Records Act below, state statutory reform should contemplate the need for identifying the “personal information” of the persons whose information has been collected into a government database.

As is provided for the President of the United States and White House staff:

Definitions

As used in this chapter—

(2) The term “Presidential records” . . .

(A) includes any documentary materials relating to the political activities of the President or members of his staff, but only if such activities relate to or have a direct effect upon the carrying out of constitutional, statutory, or other official or ceremonial duties of the President; but

(B) does not include any documentary materials that are (i) official records of an agency (as defined in section 552(e) of title 5, United States Code); (ii) personal records; (iii) stocks of publications and stationery; or (iv) extra copies of documents produced only for convenience of reference, when such copies are clearly so identified.

(3) The term “personal records” means all documentary materials, or any reasonably segregable portion thereof, of a purely private or nonpublic character which do not relate to or have an effect upon the

carrying out of the constitutional, statutory, or other official or ceremonial duties of the President. Such term includes—

(A) diaries, journals, or other personal notes serving as the functional equivalent of a diary or journal which are not prepared or utilized for, or circulated or communicated in the course of, transacting Government business;

(B) materials relating to private political associations, and having no relation to or direct effect upon the carrying out of constitutional, statutory, or other official or ceremonial duties of the President; and

(C) materials relating exclusively to the President’s own election to the office of the Presidency; and materials directly relating to the election of a particular individual or individuals to Federal, State, or local office, which have no relation to or direct effect upon the carrying out of constitutional, statutory, or other official or ceremonial duties of the President.361

Is a broader definition, such as that of the State of Washington, which defines a public record as “any writing containing information relating to the conduct of government,”362 really of superseding benefit to the public, supporting its “right to see” government,363 when a government database allows the requestor to see more of the lives of private individuals than the activity of government officials? The risks of Reverse Sunshine and unwarranted government intrusions on informational privacy should be expressly contemplated in state public records laws. Utah, for example, has made an effort to achieve this, in which its Government Records Access Management Act “was enacted to protect two constitutional rights: (a) the public’s right of access to information concerning the conduct of the public’s business; and (b) the right of privacy in relation to personal data gathered by governmental duties.”364

Finally, state and federal Public Records Acts should consider that the ordinary requestor of public records varies by level of sophistication in understanding the information contained in the record and its importance, and how the record is maintained in a Digital Age. Neither the public nor government staff should be tasked with learning all database software terminology for every government database, but they could learn the basics of database and metadata characteristics to better specify the scope of requests. For consistency and clarity, a simple government handout or website paragraph could explain the state’s definition of metadata or the reimbursement costs of

362. WASH. REV. CODE. § 42.56.010(3) (2014).
producing all or certain portions of a government database. Also, the presumption of access should not require the public to justify its need for metadata or database formatted information when public records are to be disclosed in any form. Although LexisNexis did not provide a definitive answer, subsequent state decisions and statutory reform will soon clarify whether the public can reasonably expect to obtain an electronic copy of an entire database and its accompanying metadata. The clarion call of litigants eager for access to the digital information makes this inevitable.

However, regardless of the outcome of Sunshine Law litigation in North Carolina and elsewhere, metadata and databases should not be provided in their vulnerable native formats to avoid inadvertent disclosure of protected information. Whether realistic or not, the courts clearly expect state agencies to manage appropriately and efficiently the systems they have put in place, including the need to identify and scrub or redact confidential records before public disclosure. Expecting production of hard copy printouts is also unmanageable when the information is only easily understood in its electronic format and organization. As others have discussed, there is a natural chasm in compliance between native and static formats, and there seems to be little guidance and little agreement regarding how best to manage the balance of competing policies of Sunshine Laws and confidentiality laws in the Information Age.

The problem is the public’s perception that this is an advanced Digital Age, when in fact it is a Digital Wild Frontier, not yet well prepared to manage the innovations that are rapidly being created. With respect to informational privacy, as fast as the technology is created to collect voluminous digital information, other technology is created to crack the code and discover its secrets. The North Carolina Court of Appeals in LexisNexis perhaps was most honest in this regard,

365. See supra text accompanying notes 120-21.
367. See supra Part III(A).
371. Id. at 559; see sources cited supra note 273 (citing authority in support of a trend toward judicial mandates of disclosure in native formats); see also State ex rel. Milwaukee Police Ass’n v. Jones, 615 N.W.2d 190 (Wis. Ct. App. 2000) (requiring the records custodian to provide access to original, digital 911 recordings); see also 75 Op. Wis. Atty Gen. 133, 145 (1986) (opining that refusal to provide copies of computer tapes in their electronic form would be inconsistent with the State’s public records law).
in simply stating that if the government could not manage or sustain its own technology to lawfully comply with public records requests, then it need not place public records information in databases. In other words, a prudent government body must be patient and wait until the system is fully functional, and its custodians of record fully trained to comply with public records requests.

VII. CONCLUSION

Consider government and corporate issued cameras recording images on street corners, above apartment buildings and inside office buildings, satellite recording of sound within homes, or mechanical drones surreptitiously peering through windows like flying monkeys in The Wizard of Oz. These are just some of the many real and familiar examples of the normalcy of our newly exposed life imposed upon us by governmental and commercial interests. The merging of the public and the personal into official massive public information systems, such as criminal databases and public health surveillance registries, instantly accessible across the globe, forge new opportunities for more invasive government and non-government intrusion into the lives of individuals.

Yet implementing legal restrictions protecting confidential and potentially harmful disclosure of otherwise public records becomes unwieldy in the face of public records requests for whole databases and their metadata, especially considering the paucity of legal remedies for violations. For the public to expect its state and federal governments to effectively manage massive collections of personal information regarding the lives of individuals from birth to death, protecting privacy where warranted, is simply unreasonable based on past experience and human capabilities. As noted in the introduction to the Opinion of the Advocate General for the European Court of Justice in 2013, humanity has forever valued the “right to be left alone.”

Even with experience, a system’s complexity coupled with the sophistication of hackers and the human selfishness of some employees maintaining the system, compromises the security of any online database. Clearly data mining and mass collection of information for online databases increases public access to public records, but it also invites greater disclosure of

372. See LexisNexis(Ct App), supra note 89.

373. For example, the Federal Affordable Care Act mandated electronic health records, but failed to adequately prepare technologically for the initial online purchase by the uninsured of available insurance products. See Tom Howell, Jr., Insurance Brokers See Big Problems in Obamacare Rollouts, WASHINGTON TIMES (Mar. 3, 2014), http://www.washingtontimes.com/news/2014/mar/3/insurance-brokers-see-big-problems-in-obamacare-ro/?page=all.

more forms of personal information on citizens defined as matters of public record. If the purpose of Sunshine Laws is to ensure government accountability through public access to information, then such laws should focus on government duties and functions and prohibit an overzealous sweep of government mass collection of information on individuals. The latter creates Reverse Sunshine and an increased potential for informational privacy violations, instead of a light on government corruption. The encroaching expansion of criminal justice and public health databases should concern many regarding the rights of those lives already recorded within them, and the rights of those who will be swept into the next net.

Therefore, since the choice of presenting public records in database and metadata formats has been made, it is, at minimum, time to tighten the definitions of the scope of this information as a matter of public record. With any new technological development enhancing public information access, the first task should be to carefully strengthen the privacy of individual citizens before ever permitting greater access to the public at large. State and federal courts should acknowledge this important informational privacy interest when rendering their decisions of first impression on public access to big data. Creation of government databases should be in ready form for public records requests, carefully and efficiently excluding legally protected confidential information, while metadata as a public record should be clearly defined and understood to only include information which has a direct effect on government duties.

The government has no business collecting information on private citizens for which it has no significant official use, for which taxpayers pay for its storage and maintenance, and which could then be accessed by the world as a matter of public record. Therefore, until greater care is taken in reducing the ambiguity of statutory definitions of databases and metadata as public records, and training eases the confusion of custodians of record when processing digital public records requests, the Digital Wild Frontier will persist, rendering ordinary citizens vulnerable not only to government intrusion but to the intrusion of everyone around them, all in the name of freedom of information.
APPENDIX A

HOW TO FIND PUBLIC INFORMATION

ABOUT PEOPLE ONLINE

Every year it becomes easier to track information about people online, and much of the information is free and quickly accessible. Some fee-based companies are also able to hide or bury information about you online or to tell you some of the people who have been searching for you. At the Center for Child and Family Health, access to information on the court status of cases and the criminal history of persons involved with our cases can be particularly useful. Using the free online resources below is a way for our clients and our staff to stay up to date and make safety decisions related to whether a person has been charged with a crime, arrested, has a criminal record, or to simply confirm when a court date is in a civil or criminal case. When searching, note that it is helpful if you have the person’s birth date or at least year of birth on hand, so that you can be sure you have the right record in case there are several people with the same name.

TO FIND OUT COURT DATES IN CRIMINAL AND CIVIL CASES

To find out the statewide NC criminal charges and criminal and civil court dates you can search by:
- By defendant’s (criminal) or party’s (civil) name
- Court and County
- Other means (traffic citation, law enforcement officer name, etc.)

Website: www.nccourts.org (Go to Court Calendars on right sidebar, then click on Court Calendars on left sidebar, then go to “District and Superior Court Query” on left sidebar)

TO FIND PUBLIC RECORDS ON OTHER MATTERS

Remember that many additional records are available to the public online, such as marriage, birth, death, voter registration, child support warrants for arrest, property values, and much more. County websites often have free links to these records.

For example:

---

375. This handout was developed by the author for the Legal Program at the Center for Child and Family Health in Durham, North Carolina, to assist patients, clients and staff in quickly accessing free online databases with public record information. Within the Clinical Legal Program of North Carolina Central University School of Law, the author formerly served from 2006-2014 as the Legal Director for the Center, which is a nonprofit consortium of faculty from Duke University Department of Psychiatry, University of North Carolina at Chapel Hill School of Pediatric Medicine, and North Carolina Central University School of Law focusing on medico-legal direct services and professional training.
• Durham County Public Records searches: www.dconc.gov (Government)
• Other counties, go directly to the county website or see generally: http://publicrecords.onlinesearches.com
• See also: http://pipl.com/

TO FIND WHETHER A PERSON IS IN JAIL OR PRISON
(AND THEIR CHARGES)
Jail inmates are charged with a misdemeanor or felony and are awaiting trial; serving a misdemeanor sentence; or held for a deportation hearing or transport. Prison inmates have already been convicted and are serving a felony sentence. Jails are managed by County Sheriffs, while our state prisons are managed by the NC Department of Corrections.

DURHAM COUNTY JAIL
To find out if a person is in jail or has recently been incarcerated in the Durham County Jail (within the last 30 days), including information on:

• Date confined and released; Criminal charges; Bond amount and type

Website: www.co.durham.nc.us/departments/shrf/IPS/; For immediate within the hour information, call the Booking Dept. at the Jail at: (919) 560-0772 or (919) 560-0915

JAIL INMATE INFORMATION FOR ALL COUNTIES IN NORTH CAROLINA:

http://publicrecords.onlinesearches.com/
North-Carolina-Jail-and-Inmate-Records.htm

NC DEPT. OF PUBLIC SAFETY PUBLIC ACCESS INFORMATION SYSTEM
To find out the statewide NC criminal record and history of a person convicted of a felony, and whether that person has been released from prison, including information on:

• Date of offense and conviction; County of conviction
• Crimes convicted (felonies); Sentence (including status of probation)

Website: webapps6.doc.state.nc.us/apps/offender/
SEX OFFENDER & PUBLIC PROTECTION REGISTRY IN NC 
AND OTHER STATES

To find out the registry status of a specific sex offender, OR to find out whether a registered sex offender lives near a certain address, including information on the offender’s:

- Physical description, Photo, and Home address
- Information on conviction (charge(s), date of conviction, incarceration)

Website: http://sexoffender.ncdoj.gov/ (includes general overview and state and national registries) or www.ncfindoffender.com

TO RECEIVE AUTOMATIC NOTICES OF OFFENDER STATUS, COURT DATES, AND SERVICE OF PROCESS

VINE (Victim Information Network Everyday) is part of a national network to give information to victims on when an offender is arrested, released, court dates, and when protective orders are served. Almost every county in every state in the United States takes part in this program. For an introduction to the range of what can be provided see https://www.vinelink.com/vinelink/initMap.do.

- Offender information: To register online to find inmate custody information or to receive court event notifications (telephone, email, or TTY) go to www.vinelink.com (click on NC on the map, then “Register for Notification” button, then click on “Offender” at top (not Protective Order)).
- Protective order information: The VINE system also provides automatic statewide notification of when protective orders have been served on the defendant (at which point the protective order is enforceable). To register you will need the protective order information on hand (e.g., case number, respondent’s last name, etc.). To register online go to www.vinelink.com (click on NC on the map, then “Register for Notification” button, then click on “Protective Order” at top (not Offender) and follow the instructions).

SAVAN (Statewide Automated Victim Assistance and Notification) is a free 24-hour per day notification service on changes in an offenders’ criminal status. It provides telephone, email and TTY device notices in both English and Spanish. Keep in mind telephone notification may occur at any time of day or night. Anyone may call the SAVAN hotline at 1-877-NCSAVAN (1-877-627-2826) to see if an offender is still in jail (custody status). However, by state law, only victims of crime designated for services may register for “court event” notification (e.g., the next court date). This program is sponsored by the NC Department of Public Safety. For more information go to www.ncdps.gov (Citizens, Victims of Crime) or www.ncsavans.org.
NC DEPT. OF PUBLIC SAFETY OFFICE OF VICTIM SERVICES

If you are a victim of an inmate now in prison and need help determining the status of the inmate or other matters, such as preventing unwanted contact, the NC Department of Corrections Office of Victim Services may be able to help: Contact 1-866-719-0108 (toll-free); or www.ncdps.gov (Citizens, Victims of Crime)

NATIONAL CRIMINAL AND PUBLIC RECORDS SEARCHES (FOR A FEE)

For more detailed public information, or to find out a person’s criminal history for crimes committed in other states or in the federal system, you may choose to pay for a service. The fee is in the range of $20-40 for online access to this information. An online search will quickly lead you to one of these companies, although keep in mind that most information is public record and available to you for free if you conduct your own search.

TO FIND OUT STATUS OF AN IMMIGRATION APPLICATION

Please see: https://egov.uscis.gov/cris/Dashboard.do
APPENDIX B

OFFICIAL WEB ACCESS TO DOCUMENTARY MATERIAL IN THE PRESIDENTIAL RECORDS ACT: TEXT FILE

Text File

44 U.S.C.
United States Code, 2008 Edition
Title 44 - PUBLIC PRINTING AND DOCUMENTS
CHAPTER 22 - PRESIDENTIAL RECORDS
Sec. 2201 - Definitions

§2201. Definitions
As used in this chapter—

(1) The term “documentary material” means all books, correspondence, memorandums, documents, papers, pamphlets, works of art, models, pictures, photographs, plats, maps, films, and motion pictures, including, but not limited to, audio, audiovisual, or other electronic or mechanical recordations.

(2) The term “Presidential records” means documentary materials, or any reasonably segregable portion thereof, created or received by the President, his immediate staff, or a unit or individual of the Executive Office of the President whose function is to advise and assist the President, in the course of conducting activities which relate to or have an effect upon the carrying out of the constitutional, statutory, or other official or ceremonial duties of the President. Such term—

(A) includes any documentary materials relating to the political activities of the President or members of his staff, but only if such activities relate to or have a direct effect upon the carrying out of constitutional, statutory, or other official or ceremonial duties of the President; but

(B) does not include any documentary materials that are (i) official records of an agency (as defined in section 552(e) 1 of title 5, United States Code); (ii) personal records; (iii) stocks of publications and stationery; or (iv) extra copies of documents produced only for convenience of reference, when such copies are clearly so identified.

(3) The term “personal records” means all documentary materials, or any reasonably segregable portion thereof, of a purely private or nonpublic character which do not relate to or have an effect upon the carrying out of the constitutional, statutory, or other official or ceremonial duties of the President. Such term includes—

(A) diaries, journals, or other personal notes serving as the functional equivalent of a diary or journal which are not prepared or utilized for, or circulated or communicated in the course of, transacting Government business;

(B) materials relating to private political associations, and having no relation to or direct effect upon the carrying out of constitutional, statutory, or other official or ceremonial duties of the President; and

(C) materials relating exclusively to the President’s own election to the office of the Presidency; and materials directly relating to the election of a particular individual or individuals to Federal, State, or local office, which have no relation to or direct effect upon the carrying out of constitutional, statutory, or other official or ceremonial duties of the President.

(4) The term “Archivist” means the Archivist of the United States.

(5) The term “former President”, when used with respect to Presidential records, means the former President during whose term or terms of office such Presidential records were created.


REFERENCES IN TEXT

Section 552(e) of title 5, referred to in par. (2)(B)(i), was redesignated section 552(f) of title 5 by section 1802(b) of Pub. L. 99–570.

EFFECTIVE DATE

Section 3 of Pub. L. 95–591 provided that: “The amendments made by this Act [enacting this chapter, amending sections 2111 and 2112 of this title, and enacting provisions set out as notes under this section] shall be effective with respect to any Presidential records (as defined in section 2201(2) of title 44, as amended by section 2 of this Act) created during a term of office of the President beginning on or after January 20, 1981.”

SHORT TITLE OF 1978 AMENDMENT

For short title of Pub. L. 95–591, which enacted this chapter, as the “Presidential Records Act of 1978”, see section 1 of Pub. L. 95–591, set out as a note under section 101 of this title.
SEPARABILITY

Section 4 of Pub. L. 95–591 provided that: “If any provision of this Act [enacting this chapter, amending sections 2107 and 2108 of this title and enacting provisions set out as notes under this section] is held invalid for any reason by any court, the validity and legal effect of the remaining provisions shall not be affected thereby.”

1 See References in Text note below.

2 So in original. Probably should be “thereof,”.
APPENDIX C

APPENDIX C – OFFICIAL WEB ACCESS TO THE LEGAL DEFINITION OF DOCUMENTARY MATERIAL IN THE PRESIDENTIAL RECORDS ACT: DESCRIPTIVE METADATA (MODS)\(^{377}\)

**DESCRIPTIVE METADATA (MODS)**

This XML file does not appear to have any style information associated with it. The document tree is shown below.

```xml
  <name type="corporate">
    <namePart>United States Government Printing Office</namePart>
  </name>
  <name type="corporate">
    <namePart>United States</namePart>
    <namePart>Congress</namePart>
    <namePart>House of Representatives</namePart>
    <namePart>Office of the Law Revision Counsel</namePart>
  </name>
  <typeOfResource>text</typeOfResource>
  <genre authority="marcgt">government publication</genre>
  <description>Government Organization</description>
</mods>
```

Section 552(e) of title 5, referred to in par. (2)(B)(i), was redesignated section 552(f) of title 5 by section 1802(b) of Pub. L. 99-570.

Section 3 of Pub. L. 95-591 provided that: “The amendments made by this Act [enacting this chapter, amending sections 2111 and 2112 of this title, and enacting provisions set out as notes under this section] shall be effective with respect to any Presidential records (as defined in section 2201(2) of title 44, as amended by section 2 of this Act) created during a term of office of the President beginning on or after January 20, 1981.”
APPENDIX D

OFFICIAL WEB ACCESS TO THE LEGAL DEFINITION OF DOCUMENTARY MATERIAL IN THE PRESIDENTIAL RECORDS ACT: AUTHENTICITY METADATA

AUTHENTICITY METADATA (PREMIS) (IN PART)

This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
  <object xsi:type="representation">
    <objectIdentifier>
      <objectIdentifierType>FDsys AIP</objectIdentifierType>
      <objectIdentifierValue>R0b002ee180b76c0b</objectIdentifierValue>
    </objectIdentifier>
  </object>
  <object xsi:type="file">
    <objectIdentifier>
      <objectIdentifierType>FDsys AIP</objectIdentifierType>
      <objectIdentifierValue>D09002ee180b76c15</objectIdentifierValue>
    </objectIdentifier>
    <objectCharacteristics>
      <compositionLevel>0</compositionLevel>
      <format>
        <formatDesignation>
          <formatName>application/pdf</formatName>
        </formatDesignation>
      </format>
    </objectCharacteristics>
  </object>
  <object xsi:type="file">
    <objectIdentifier>
      <objectIdentifierType>FDsys AIP</objectIdentifierType>
      <objectIdentifierValue>D09002ee180b76c14</objectIdentifierValue>
    </objectIdentifier>
    <objectCharacteristics>
    </objectCharacteristics>
  </object>
</premis>
```

A WORLD INFORMATION ORDER — PRIVACY AND SECURITY
IN A HYPER-NETWORKED WORLD OF DATA AND ANALYSIS

Michael Losavio, Youngjin Song, Joshua I. James,
Andrew Marrington, K.P. Chow

ABSTRACT

We now live in a new space of information density, evolving with the
Internet of Things and the Smart City. This global information space is shared
with powerful analytics that can give an organization, private or public, massive
surveillance powers. As Justice Sotomayor commented in United States of
America v. Jones (2012), this may change the relationship between government
and the governed.

Technical security cannot protect privacy and security with such a data life,
but requires a security, assurance and privacy regime that encompasses all
domains of society. The challenge will be to establish a balance of these elements
in a contentious and dangerous world.

We examine the evolving facts and law relating to personal autonomy,
identity and authenticity of electronic data, its mutability and evanescence, and
how this might impact the liberties and security of the peoples of the world.

I. INTRODUCTION

THE NEW SPACE OF INFORMATION DENSITY, ITS RISKS AND RIGHTS

A new space of information density evolves with the Internet of Things and
the Smart City.1 This comes as a sensor-ridden world generates masses of data
that are collected and analyzed by more and more powerful programs. With
relatively little effort and cost, it gives every government and data aggregator the
potential surveillance powers of totalitarian regimes that, in the past, directed
huge resources to surveil their citizens.2 This surveillance and predictive power

* Michael Losavio, University of Louisville, U.S.A.; Youngjin Song, International
Cybercrime Research Center, Korean National Police University, Republic of Korea; Joshua I.
James, Digital Forensic Investigation Research Laboratory, Hallym University; Chuncheon,
Republic of Korea; Andrew Marrington, Zayed University, Dubai, U.A.E.; K.P. Chow, University
of Hong Kong, Hong Kong SAE, Peoples Republic of China.

** Acknowledgments: We thank Brian Morris and Michael Enzweiler for their crucial
editorial and research support.

1. Mary Branscombe, How the Internet of Things Makes Cities Smart, TechREADY (Apr. 4,
makes-cities-smart-1239908.

2. Tom Risen, Futurology: Internet of Things and the NSA, U.S. NEWS & WORLD REPORT
can both enhance community security and create new threats to the privacy and personal autonomy of everyone.3

The “Smart City” reflection of the “Internet of Things” focuses on the city and the kinds of information that may be collected from the embedded, networked devices within the people and artifacts in that city. That data from activities with the city can be analyzed to better deliver city services. IBM’s paradigm for this is a community of people, places and things that are each instrumented, interconnected and “intelligent,” i.e., computationally-adapted.4

The paradigm is straightforward, with technology permitting embedded computing and communication systems in and on things and persons that link then to other, broader networks for the exchange and analysis of the data.5 One example is the growth of global positioning satellite (GPS) geotagging of activity that can be transmitted and collected, from which it can be analyzed.6 Such analysis includes visualization of the daily life of someone in constant geotagging contact.7 It can help improve such essential public services as traffic control, crowd monitoring and crime prevention.

But Associate Justice Sonia Sotomayor noted in her concurring opinion in GPS tracking case of United States v. Jones (2012) that this may come with a price. Justice Sotomayor opined that ubiquitous computing across ever more dense matrices of communication simply changes how we might know things that, in the past, might be beyond easy knowledge.8 Such use might yet conflict with the proper boundaries of state action “when the government violates a subjective expectation of privacy that society recognizes as reasonable.”9 She observed as to the interconnected sensors of radio-linked global positioning satellite (GPS) monitors analyzed with geo-mapping and locational computing that:

In cases involving even short-term monitoring some unique attributes of GPS surveillance relevant to the Katz analysis will require particular attention. GPS monitoring generates a precise, comprehensive record of a person’s public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations. See, e.g., People v. Weaver, 12 N.Y. 3d 433, 441–442, 909 N. E. 2d 1195,
1199 (2009) ("Disclosed in [GPS] data . . . will be trips the indisputably private nature of which takes little imagination to conjure: trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on"). The Government can store such records and efficiently mine them for information years into the future. Pineda-Moreno, 617 F. 3d, at 1124 (opinion of Kozinski, C. J.). And because GPS monitoring is cheap in comparison to conventional surveillance techniques and, by design, proceeds surreptitiously, it evades the ordinary checks that constrain abusive law enforcement practices: “limited police resources and community hostility.” Illinois v. Lidster, 540 U.S. 419, 426, 124 S. Ct. 885, 157 L.Ed.2d 843 (2004).10

Even the awareness of such potential logging of one’s positional life might have a deterrent, chilling effect of a person’s actions even for protected rights of association, publication and expression.11 Such immense private information offers immense power for which there are few current limits on misuse.12

At the heart of the Smart City paradigm and Justice Sotomayor’s concerns is aggregated and easily analyzed information.13 The instrumented/interconnected/intelligent alliterative model creates just such information from widely disparate sources which, with the proper reflection, become knowledge about people.14 The knowledge itself may depend on the source of the data (point-of-sale, clothing RFID tags, vehicle ID), the types of data (time, location, content), the aggregations and collections and their scope, location and control, the computational reach of the data analytics and the ultimate use to which that knowledge may be put.15 Systems may chose the particular transactional point or space, such as a person or group, recreation or vocation, or supporting or mediating services.16

There may be great benefits from such a dense, shared information space. “Smart” traffic control, for example, may optimize transportation without the

11. Id. at 956.
12. See id.
15. See Chamberlin, supra note 13.
immense cost of new road infrastructure.\textsuperscript{17} A person always knows the good
restaurants nearby. Or where friends might be. Conversely, no traffic infraction
goes unnoticed, nor a stalker’s opportunity.

The spheres of data deserving and given protection vary between states.\textsuperscript{18}
They include the sphere of family life, hybrid areas of expected protection, by
tradition, constitution or statute, and spheres of public and limited-public
interaction with third parties.\textsuperscript{19}

The security and privacy issue is especially significant for the protection of
people from others, whether miscreants or the state.\textsuperscript{20} This invokes issues as to
personal autonomy, identity and authenticity.\textsuperscript{21} These may be impacted in
different, unexpected and unanticipated ways.

\textbf{II. THE NEW COMPUTATIONAL WORLD OF
HIGH-POWERED ANALYTICS – RISKS AND RIGHTS}

Computational systems, properly used and understood, can greatly enhance
the effectiveness of standard forensic techniques by efficiently applying
probability analysis and pattern matching to enhance reliability.\textsuperscript{22} These
techniques, once validated, may be applied with far greater consistency as to
assure reliable results without the risk of human error.\textsuperscript{23}

But forensic analysis has been broadly criticized for lack of rigorous and
mandatory certification programs for forensic analysts, strong standards and
protocols for analyzing and reporting on evidence and peer-reviewed, published
studies establishing the scientific bases and reliability of many forensic

\begin{flushright}
17. Joshua Barrie, \textit{Here’s How The Internet of Things Will Solve Traffic Jams And Take The
Stress Out Finding A Parking Space}, BUS. INSIDER (Jan. 27, 2015, 10:20 AM),


19. See generally Meg Leta Ambrose, \textit{It’s About Time: Privacy, Information Life Cycles, And

20. Id. at 382–85.

21. See id.

SPECTRUM (Nov. 29, 2010), http://spectrum.ieee.org/computing/software/
beyond-csi-the-rise-of-computational-forensics. The discipline of Computational Forensics
(CF) has been described as an emerging interdisciplinary research domain. See K. Franke &
S.N. Srihari, \textit{Computational Forensics: Towards Hybrid-Intelligent Crime Investigation, in
IAS 2007 THIRD INTERNATIONAL SYMPOSIUM ON INFORMATION ASSURANCE AND SECURITY
383–86 (2007). 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. Id. 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. Id.

\end{flushright}
methods.24 These characteristics assure reliability and are considered by judicial
gatekeepers as to permitting use of such evidence, whether for trial, issuance of a
search warrant or order, or punishment.25

The human factor also plays a significant role impacting reliability, as
forensic validation must examine “the extent to which practitioners in a particular
forensic discipline rely on human interpretation that could be tainted by error, the
threat of bias, or the absence of sound operational procedures and robust
performance standards.”26

A secure life means safety in the world, from all comers. It is both physical
and informational safety. They range from respect for personal autonomy in
image and confidences to data assurance for correct and safe judgments on a
course of action. Damage may be physical, such as an assault from a cyber-
stalker or state officer executing an arrest. Damage may be to liberty interests,
such as the right to be free of detention and imprisonment. And it may be
informational, such as intentional or negligent defamation or revelations as to
intensely private matters. All of these interests are protected, to one extent or
another, and contribute to how people live and work with others. It is living and
working in the hyper-instrumented, hyper-networked world that stresses these
interests and obligations to protect them.

This information world creates opportunities for misconduct that necessitate
new investigative methods. Computational systems aid in the effective
investigation of distributed misconduct, particularly with the ubiquitous use of
computing systems.27 Contraband exchange and distribution over the Internet
might be investigated and prosecuted in a cost-effective manner with such
systems using relational probabilistic inference.28 Yet this also allows easy, low
cost monitoring of all activities of those using these systems for any purpose.29

24. See Nat’l Acad. of Sci. Comm. on Identifying the Needs of the Forensic Cmty.,
25. See generally Daubert v. Merrill Dow Pharmaceuticals, Inc., 509 U.S. 579 (1993); see
also Fed. R. Evid. 702 (providing that the trial judge ensure that any and all scientific testimony or
evidence admitted is not only relevant, but reliable).
27. See generally Michael Losavio, Deborah Keeling & Michael Lemon, Models in
Collaborative and Distributed Digital Investigation: In the World of Ubiquitous Computing and
28. See generally Jennifer L. Wong et al., Computational Forensic Techniques for Intellectual
Circuits and Systems 894 (2004); see also Matei Ripeanu et al., Mapping the Gnutella Network:
Properties of Large-Scale Peer-to-Peer Systems and Implications for System Design, in 6 IEEE
Internet Computing 50–57 (2002); see also Michael Losavio et al., Node-Based Probing and
Monitoring to Investigate Use of Peer-to-Peer Technologies for Distribution of Contraband
Material, in Third International Workshop on Systematic Approaches to Digital Forensic
29. See Wong, supra note 28.
And given the networked world and global engagement, multiple jurisdictions may be impacted by the use of some computational systems for investigation. Avoiding violations of particular national laws may require additional effort; this is especially true with cloud computing systems and services that may be accessed from and hosted in multiple places anywhere on the globe.

The evidence continuum requires assessments of reliability, whether for use in commerce, investigation, proof of guilt or appropriateness of punishment. The commerce - forensic link has long been a part of evidentiary vetting under the “business records” exception to the prohibition on use of unreliable hearsay. Again, these rules may vary with jurisdiction and may require consideration of the laws of the states of data collection, transmission and analysis together, such as where there is transnational collaboration between state officers.

III. COMPUTATIONAL AND DATA ANALYTICS

With a world instrumented and interconnected, all that data is now ready for analysis. Computational techniques may include informational retrieval, case-based reasoning, and probabilistic/Bayesian systems, but not without challenge.

It is ironic that the main restriction on the efficacy of ubiquitous sensor networks and other data collection mechanisms as a mechanism for mass surveillance is in fact that, at the present time, we lack the technical capability to practically analyze the volume of data we collect. Instead, this massive quantity of collected data, i.e. big data, exists primarily as a bank from which relevant records pertaining to an investigation or other proceedings may be retrieved and analyzed as required. In other words, due to the present technical limitations, only a subset of the collected data can ever be practically analyzed. In some investigations, identifying that subset is relatively straight forward, but in others the task is more challenging. It is long acknowledged in the digital forensics

34. See generally Steven H. Thiesen, Evidence Seized in Foreign Searches: When Does the Fourth Amendment Exclusionary Rule Apply?, 25 WM. & MARY L. REV. 161 (1983); see also United States v. Verdugo-Urquidez, 494 U.S. 259, 261 (1990) (holding that the Fourth Amendment does not apply to the search and seizure by United States agents of property owned by a nonresident alien and located in a foreign country).
literature that the increasing volume of storage media poses a challenge for digital investigations, because the process of examining all of this data and identifying relevant evidence remains largely manual, requiring new techniques in order to bring investigations to a timely conclusion. In effect, these emerging digital forensics techniques, such as triage, seek to identify the subset of data involved in a case which might actually be interesting to the investigator. Similarly one can see that it will be necessary to restrict the quantity of data to be analyzed in cases involving information gathered from the myriad devices of the Internet of Things to only that data which are most relevant. This will not only be necessary from a privacy perspective, but also from a technical perspective, in order to best facilitate the analysis of data relevant to an investigation.

One example of concerns with these systems may be seen in one court’s concerns over the effectiveness of information retrieval (IR) algorithms:

Whether search terms or “keywords” will yield the information sought is a complicated question involving the interplay, at least, of the sciences of computer technology, statistics and linguistics. See George L. Paul & Jason R. Baron, Information Inflation: Can the Legal System Adapt?, 13 RICH. J.L. & TECH. 10 (2007). Indeed, a special project team of the Working Group on Electronic Discovery of the Sedona Conference is studying that subject and their work indicates how difficult this question (**24) is. See The Sedona Conference, Best Practices Commentary on the Use of Search and Information Retrieval, 8 THE SEDONA CONF. J. 189 (2008), ... Given this complexity, for lawyers and judges to dare opine that a certain search term or terms would be more likely to produce information than the terms that were used is truly to go where angels fear to tread. ...

Data analytics via probabilistic and statistical methods are at the extreme edge of analysis as it may impact lives. Analytics in commercial enterprises are immensely powerful engines for inferences on a person. The analytics may look at statistical analyses and frequentist or Bayesian probability for inferential conclusions. These analytics naturally transfer to other areas of human endeavor, particularly public security and the administration of justice. Many commentators have expressed concern as to the use in system of justice, including for inferences, reliability, relevance, weight and proof.

The attempted application of a statistical model to estimate contraband quantity so as to appropriately punish a smuggler was rejected as fictive and not

---

“specific evidence” of drug quantities carried by the defendant, as the model was inadequate and failed to examine needed relevant variables and dependencies.\textsuperscript{38} Indeed, as noted by the court below “dependencies are especially likely to be found in problems involving a sequence of similar human actions,” but, nonetheless, the model, being built on “...the extrapolation for the prior seven trips [that] was based on what 117 other people had done” was flawed, did not represent “specific evidence” of misconduct and warranted remand.\textsuperscript{39, 40}

In the future, however, advances in data analytics will permit, from a technical perspective at least, meaningful analysis not just of a limited subset but of the whole set of the data collected about an individual. Beyond the purposes of law enforcement and surveillance, big data is being collected in the commercial world to provide business intelligence. The techniques being developed today to optimize advertising and predict market trends may, in the future, be adapted to the analysis of big data sets collected with surveillance in mind. While technical limitations today mean that only small, highly relevant parts of this big data can be feasibly analyzed as part of any given case, this will not be the case forever.

Reliability, relevance and weight will be continued concerns for the use of the results of these systems in the administration of justice.\textsuperscript{41} Their use against privacy and peoples must also be weighted. It is a significant challenge in a globally-connected world.

IV. United States

A. Criminal Justice Issues in Mercantile, Investigative and Forensic Computation

The U.S. Supreme Court’s ruling in the GPS tracking case United States v Jones barred such technology without the permission given by a search warrant where a neutral, third-party magistrate reviewed sworn facts and found probable cause that use would lead to evidence of a crime. The reasoning hearkened back to trespass doctrine in the placement of a device on a target vehicle, an invasion sufficient to make the “search” unreasonable even though the vehicle could have properly been placed under surveillance and followed by investigators. But Justices Sotomayor and Alito noted the unparalleled ease of surveillance of anyone with the technology, which would track, collect and analyze a person’s vehicular movements at little cost; they suggested analysis of the reasonableness of the use of such power to monitor the lives of others.

\textsuperscript{38} United States v. Shonubi, 103 F.3d 1085 (2d Cir. 1997).
\textsuperscript{40} Shonubi, 103 F.3d at 1091.
A parallel question of the reasonableness of expectations of privacy in a person’s personal data collections was addressed in 2014 in *Riley v. California* and *United States v. Wurie*, where the Supreme Court held that simply finding a cellular telephone on an arrestee did not, alone, justify searching the phone and its contents absent a warrant and a finding of probable cause of criminal artifacts, whether as evidence or instrumentality, in relation to it. The import here of the device, as opposed to papers, was the type and huge amount of information it might maintain on a person’s personal life and affairs. It was necessary to weigh “by assessing, on the one hand, the degree to which it intrudes upon an individual’s privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests.” The technology itself risked neither danger nor loss of evidence that outweighed the privacy interests in the large and diverse data it contained.

Probabilistic and inferential practice is deeply embedded in American criminal justice. The Fourth Amendment protects “[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures. . . .” The requirement of “probable cause” requires a determination or inference of reliability that is key to any evidence. That blocks unbridled discretion by police officers in searching and seizing individuals. A person may be arrested without a warrant only on probable cause. That arrest is permissible only if there is probable cause based “the totality of the circumstances” that felony has been or is being committed by the person arrested.

With either the existence of “reasonable suspicion” or “probable cause,” the determination as to the existence of either rests on 1) a determination of the historical facts leading up to the seizure and 2) a mixed question of law and fact as to whether those historical facts, considered by a reasonable police officer, amount to a reasonable suspicion or probable cause of criminal activity.

A police officer cannot arrest someone absent probable cause, i.e., a “fair probability” that the individual has either committed or intends to commit a crime. Probable cause “…is a fluid concept-turning on the assessment of

43. Id.
44. Id. (citing Wyoming v. Houghton, 526 U.S. 295, 300 (1999)).
45. U.S. Const. amend. IV.
probabilities in particular factual contexts – not readily, or even usefully, reduced to a neat set of legal rules. 52

As the Supreme Court noted in Brinegar v. United States, 338 U.S. 160, 175 (1949):

In dealing with probable cause, however, as the very name implies, we deal with probabilities. These are not technical; they are the factual and practical considerations of everyday life on which reasonable and prudent men, not legal technicians, act. The standard of proof is accordingly correlative to what must be proved.

‘The substance of all the definitions’ of probable cause ‘is a reasonable ground for belief of guilt.’ McCarthy v. De Armit, 99 Pa. 63, 69, quoted with approval in the Carroll opinion. 267 U.S. at page 161, 45 S.Ct. at page 288, 39 A.L.R. 790. And this ‘means less than evidence which would justify condemnation’ or conviction, as Marshall, C.J., said for the Court more than a century ago in Locke v. United States, 7 Cranch 339, 348. Since Marshall’s time, at any rate, it has come to mean more than bare suspicion: Probable cause exists where ‘the facts and circumstances within their (the officers’) knowledge and of which they had reasonably trustworthy information (are) sufficient in themselves to warrant a man of reasonable caution in the belief that’ an offense has been or is being committed. Carroll v. United States, 267 U.S. 132, 162 , 288, 39 A.L.R. 790. 53

The issue then is how computational results may support legal action.

In the context of digital and network forensics, this has implications for the data quantum needed for a search warrant to enter a home or business and seize the devices found that. Several courts have found that email addresses, personal names and credit card numbers on contraband servers show this “fair probability” of illegal activity. 54

Computational analysis plays a major role in federal criminal law in the United States via its implementation in the United States Sentencing Guidelines. 55 Criticism of the Guidelines reflects conflicts over the use of inference and proof derived from mathematical and probabilistic methods for legal reasoning and judgments, including Bayesian and frequentist statistical

inferences, with which courts struggle. Arguably this has been corrected by Supreme Court rulings that these guidelines are only advisory, with sentencing courts free to make individual sentences. But these guidelines are still given a “presumption” of “reasonableness” that, while not necessarily strong, is without any weighting to permit a sentencing court to fully and understandably apply them.

The private use of such power presents its own issues. Private parties may themselves build profiles of individuals and their lives some might consider inappropriate intrusions into privacy. These data aggregators may, in turn, sell this information to other parties. One of the largest U.S. commercial data brokers was the subject of Federal Trade Commission action for failing to adequately protect its data on consumers. But as to the intrusiveness of data analytics and the transfer of such analysis there are few protections available for U.S. citizens. This is in contrast with the European Union privacy directive that offers protections for individuals as to private and commercial analysis and transfer of such information. There has been limited data privacy legislation protecting video rental and drivers’ license records, in response to perceived abuses. It is possible there will be a more comprehensive regime for privacy protection in computational data by private and commercial interests as public concern over these issues grows.

V. FEDERAL REPUBLIC OF GERMANY

In the aftermath of Edward Snowden’s revelations on the scope of electronic surveillance by the U.S. National Security Agency, Federal Republic of Germany expanded efforts to strengthen cybersecurity in Germany as a whole, while

59. See Baron-Evans, supra note 55, at 13, 18.
60. Id.
continuing its effort to protect privacy both in domestic and international levels.\textsuperscript{66} This section briefly describes German federal intelligence services and oversight bodies, the legal basis of national program for mass surveillance and the recently proposed draft cyber security law.

A. Intelligence Activities and Oversight

Three intelligence services exist at the federal level: The Federal Intelligence Service (Bundesnachrichtendienst or BND), the Federal Office for the Protection of the Constitution (Bundesamt für Verfassungsschutz or BfV), and the Military Counterintelligence Service (Militärischer Abschirmdienst or MAD).\textsuperscript{67} The BfV and MAD are domestic intelligence services which is tasked with “intelligence-gathering on threats concerning the democratic order, the existence and security of the federation or one of its states, and the peaceful coexistence of peoples; with counter-intelligence; and with protective security and counter-sabotage,”\textsuperscript{68} whilst the BND is responsible for conducting foreign intelligence analysis and electronic surveillance of “threats to German interests” from abroad.\textsuperscript{69} In addition, it should be noted that there are also domestic intelligence services at the level of the federal state, the state offices for the protection of the constitution (Landesämter für Verfassungsschutz or LfV).\textsuperscript{70}

In order to control the activities of German intelligence services, there are two oversight bodies of the German Parliament.\textsuperscript{71} Firstly, there is the Parliamentary Control Panel (Parlamentarisches Kontrollgremium or PKGr).\textsuperscript{72} The German government is obliged to inform the PKGr and to provide all relevant information on the activities of the intelligence agencies to its members.\textsuperscript{73} The PKGr consists of 11 Members of Parliament and is involved in political oversight.\textsuperscript{74} Secondly, there is the G10 Commission (G10 Kommission).\textsuperscript{75} The G10 Commission discusses the legitimacy of intervention


\textsuperscript{67} Id. at 68.

\textsuperscript{68} Id.

\textsuperscript{69} Id.

\textsuperscript{70} LUDWIG GIES, GERMAN LAWS GOVERNING PARLIAMENTARY CONTROL OF INTELLIGENCE ACTIVITIES 5-6 (2010).

\textsuperscript{71} BIGO, supra note 66, at 72.

\textsuperscript{72} Id.

\textsuperscript{73} Id.


\textsuperscript{75} BIGO, supra note 66, at 72.
into Article 10 of the German Basic Law. Its monitoring activities are composed not only of reviewing ministerial instructions to perform surveillance measures, but also of collecting, processing and utilizing personal data gathered by the intelligence services, as well as deciding on whether to inform those affected. Any activities that interfere with the privacy of correspondence, posts, and telecommunications are subject to the approval of the G10 Commission.

B. Legal Framework of National Program for Mass Surveillance of Personal Data

Article 10 of the Basic Law for the Federal Republic of Germany (hereinafter “Basic Law”) on the privacy of correspondence, posts and telecommunications states that

1. The privacy of correspondence, posts and telecommunications shall be inviolable.

2. Restrictions may be ordered only pursuant to a law. If the restriction serves to protect the free democratic basic order or the existence or security of the Federation or of a Land, the law may provide that the person affected shall not be informed of the restriction and that recourse to the courts shall be replaced by a review of the case by agencies and auxiliary agencies appointed by the legislature.

The main federal law in Germany regulating communications surveillance is the “Act Restricting the Privacy of Correspondence, Posts and Telecommunications (Hereinafter “G10 Act”), which allows for certain limitations to the secrecy of communications as provided in the Article 10 of the Constitution. Under the G10 Act, intelligence services may operate, without warrant, automated wiretaps of domestic and international communications for specific purposes such as the fight against terrorism or the protection of the Constitution. Also, the act in its Section 10, Para 4 allows the BND to search up to 20% of foreign communications according to certain keywords.

76. Id.
77. Id.
80. Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses in der Fassung des Gesetzes zur Änderung des Strafgesetzbuches, der Strafprozeßordnung und anderer Gesetze (Verbrechensbekämpfungsgesetz), at 3186 (Oct. 28, 1994) (Crime Control Act) (in German); see also geändert durch das Begleitgesetz zum Telekommunikationsgesetz (BegleitG), at 3108 (Dec. 17, 1997) (Accompanying the Telecommunications Act) (in German).
81. Id.
82. Id.
The G10 Act was amended in 1994 and expanded the Federal Intelligence Service’s authority to conduct telecommunication surveillance.\textsuperscript{83} Pursuant to the amendments to the G10 Act, the newly added justifications for telecommunication surveillance targeted the burgeoning use of wireless technology and were global in their scope.\textsuperscript{84} Additionally, the amendments to the G10 Act removed the previous prohibition on sharing collected intelligence with other agencies, opening the door for the use of the shared intelligence in criminal prosecutions.\textsuperscript{85}

Two major decisions of the Federal Constitutional Court have limited the scope of the G10 Act in recent years.\textsuperscript{86} In the \textit{Acoustic Surveillance Case} in 2004, the Court upheld the 1998 amendments to Article 13 of the Basic Law that permitted acoustic surveillance of the home.\textsuperscript{87} The home provides a secure sphere for the most personal and intimate communication.\textsuperscript{88} The Court concluded that the importance of the degree of privacy granted to a home justifies attributing nearly absolute protection that no government may infringe.\textsuperscript{89} In 2008, in a landmark decision (\textit{Online Search Case}), the Court invalidated the “online search” provisions in the newly amended Constitutional Protection Act passed by the state of North Rhine-Westphalia.\textsuperscript{90} The Court interpreted Articles 1 and 2 of the Basic Law as containing a fundamental right for every citizen to have the integrity and confidentiality of information technology systems guaranteed by the state.\textsuperscript{91}

\textbf{C. Draft IT Security Act}

On 19th August 2014, the German Federal Ministry of the Interior presented a draft legislation that introduces mandatory cyber security measures designed to ensure the protection of IT systems.\textsuperscript{92} The Draft IT Security Act (the “Draft Act”)\textsuperscript{93} is part of the Federal Government’s “Digital Agenda 2014-2017”, a

\begin{itemize}
  \item \textsuperscript{84} \textit{Id.} at 381.
  \item \textsuperscript{85} \textit{Id.} at 382.
  \item \textsuperscript{86} \textit{Id.} at 383-84.
  \item \textsuperscript{87} \textit{Id.} at 383.
  \item \textsuperscript{88} \textit{Id.}
  \item \textsuperscript{89} 109 BVerfGE 279, at 313-314 (2004) (in German).
  \item \textsuperscript{90} 120 BVerfGE 274 (2008) (in German).
  \item \textsuperscript{91} \textit{BIGO}, \textit{supra} note 66, at 71.
  \item \textsuperscript{92} \textit{See} Entwurf eines Gesetzes zur Erho\'hung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) 6 (IT Security Act), \textit{available at} http://www.bmi.bund.de/SharedDocs/Downloads/DE/Nachrichten/Kurzmeldungen/entwurf-it-sicherheitsgesetz.pdf?jsessionid=5274A3C400091FB2745DF057166A929.2_cid295?__blob=publicationFile (in German); \textit{also available at} http://www.bmi.bund.de/SharedDocs/Downloads/EN/Broschueren/2014/digital-agenda.pdf?__blob=publicationFile (in English).
  \item \textsuperscript{93} \textit{Id.}
\end{itemize}
program of the German government to strengthen the position of Germany in the field of information technology.\textsuperscript{94}

The draft legislation proposes minimum organizational and technical security standards of critical infrastructures providers and an obligation to report “significant IT security incidents.”\textsuperscript{95} However, the draft Act also proposes measures to further strengthen cyber security in Germany as a whole.\textsuperscript{96} The Act would require public telecommunications networks and Internet service providers to raise security standards.\textsuperscript{97}

Furthermore, the draft includes provisions on raising the level of protection for federal information technology; strengthening the Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik, or BSI); and expanding the competences of the Federal Criminal Police Office (Bundeskriminalamt, or BKA), particularly in cases of cyber attacks on nationwide structures.\textsuperscript{98}

In addition to the draft legislation, German government has been actively supporting the discussion processes in the UN Human Rights Council and the UN General Assembly (including a German-Brazilian initiative entitled “The right to privacy in the digital age”).\textsuperscript{99} In response to the Snowden revelations, Germany and other countries, including France, Russia, Brazil and Indonesia, have submitted a draft resolution on the right to privacy in the digital age to the UN General Assembly.\textsuperscript{100} In November 2014, the Third Committee (Social, Humanitarian and Cultural) of the United Nations General Assembly approved, without vote, a draft resolution on the right to privacy in the digital age.\textsuperscript{101} The resolution calls upon all states to take measures to put an end to violations of this right, and to establish independent national oversight mechanisms capable of ensuring transparency and accountability of State surveillance of communications, their interception and collection of personal data.\textsuperscript{102}

\textsuperscript{94} Id.
\textsuperscript{95} Id. at 3.
\textsuperscript{96} Id. at 4.
\textsuperscript{97} Id. at 4.
\textsuperscript{99} \textit{DIE BUNDESREGIERUNG, Digital Agenda}, at 36 (2014).
\textsuperscript{102} Id. at 4.
VI. COMMONWEALTH OF AUSTRALIA

The Australian Parliament passed legislation to require telephony and Internet service providers to retain metadata about the communications of their customers for two years. 103 Criminal law enforcement agencies will be able to obtain access to this information with a warrant; the metadata must otherwise be kept confidential by the service provider, who is obliged to keep it encrypted and protect it from unauthorized access or modification. 104 The legislation does not require the content of the communications to be retained; it defines metadata as encompassing information about the customer’s subscription and devices, source and destination of the communication, date and time of the communication, physical location of the device initiating the communication, and the type of communication (e.g. email, social media, SMS). 105 Although the legislation requires that criminal law enforcement agencies obtain a warrant to access the collected metadata, its passage has been controversial. 106

Privacy advocates are concerned that this data retention scheme constitutes mass surveillance of the Australian population.

VII. REPUBLIC OF KOREA

A. Korean History Influencing Modern Day Privacy Issues

Korea has a long history, in which the Republic of Korea is a very new concept. The beginnings of Korea were based on kingdoms that were heavily influenced by Chinese philosophy, trade and tribute. 107 Prior to a Republic, the Joseon (조선) Dynasty [1392-1897] – an extremely Neo-Confucian society – came to power. 108 This Neo-Confucian philosophy continues to greatly influence the language and way of thinking of Koreans today.

After World War II ended, South Korea had a Military Government controlled by the United States Military. 109 The first Republic of Korea was created in 1948 but in 1961 became a Military Dictatorship when Park Chung-hee took power. 110 Although Korea became a Republic again in 1972, Park

104. Id.
105. Id. at 2.
106. Id. at 4 (discussing how the amendment is meant to limit the power to obtain warrants).
110. Id.
Chung-hee held power until his assassination in 1979. Korea worked to stabilize the democratic system, and the first free election was held in 1987. This no-so-distant history, has a number of implications for Korea’s approach to cyber security and privacy. In Korean Confucianism, every person has a rank in society, and lower ranking individuals must show respect to higher ranking individuals. This often translates to a very military-like, one-way communication down the chain of command. In reality this system makes it very difficult for an average person to have their opinions recognized. This in turn makes people less likely to openly express their opinions and especially criticisms.

During Japanese and Korean military dictatorship, Koreans who stood up against the governing power were tortured and murdered. Effectively, Koreans were told that people should not oppose the “ruling party”, or political party that is currently represented by the president. Much of the centralized power created during the military dictatorship has not been redistributed. Power is especially concentrated with the President and the National Intelligence Service (NIS), the latter having no practically effective oversight or auditing save for the President.

At a practical level the Republic of Korea has been a democracy only since 1987, and is still very much developing. Many Koreans still remember the military dictatorship, and received education indoctrinating such ideals. Combined with a Confucian culture, the result is that the democratic procedure may be similar to other democratic countries, but the conceptualization and practice of democracy in Korea is still somewhat similar to a King or Dictator, although an elected one.

B. Cyber Crime and Cyber Terrorism

Korea benefits from a modern, high-speed Internet infrastructure. In 1997 the Korean National Police established the Computer Crime Investigation Squad, which later expanded to form the Cyber Terror Response Center (CTRC), with over 900 sworn officers and civilians dedicated to cyber crime investigation and support. The Prosecutor’s Office, the Republic of Korea Armed Forces, and the National Intelligence Service also have investigation authority in this area.

111. Id.
112. Id.
113. Id.
115. SAVADA, supra note 109.
116. Id.
All of these organizations are actively building capacity to conduct cyber-related investigations and operations.\footnote{118}{See generally ROBERT DEIBERT ET AL., ACCESS CONTESTED (2011).}

Because of the lack of definition relating to cyber crime and cyber-warfare, multiple organizations may claim authority over a particular case, resulting in political conflicts between each group. These conflicts eventually escalated, until the proposal of the South Korean National Cyber Terrorism Prevention Act (“Korean National Cyber Terrorism Prevention Act,” 2013) (the Act).\footnote{119}{South Korean National Cyber Terrorism Prevention Act, CYBERCRIME TECH., http://www.cybercrimetech.com/2013/04/south-korean-national-cyber-terrorism.html (last visited June 7, 2015) (in Korean).} This act was backed by the NIS, and effectively gave control of all cyber attack related response to a centralized ‘Cyber Control Tower’ directed by the National Intelligence Service with oversight by the President.\footnote{120}{Id.} The Act also allows the NIS to force private organizations to share data ‘for the detection and prevention of cyber attacks’.\footnote{121}{Id.}

The Act itself provides very little in terms of oversight for actions taken, and when such powers can be enacted.\footnote{122}{Id.} The Act is also controversial due to financial ties between its supporters and the NIS as well as timing in relation to cyber attacks, especially ‘Dark Seoul’\footnote{123}{Lee Minji, Gov’t confirms Pyongyang Link in March Cyber Attacks, YONHAP NEWS AGENCY (Apr. 10, 2013, 3:54 PM), http://english.yonhapnews.co.kr/northkorea/2013/04/10/49/0401000000AEN20130410007352320F.HTML.} which – based on weak evidence – helped the NIS to show a North Korean element to cyber attacks, helping to prove cyber security is a national security issue.\footnote{124}{A Wake-Up Call to S. Korea About Cyber Security, YONHAP NEWS AGENCY (Mar. 28, 2013, 6:01 PM), http://english.yonhapnews.co.kr/yhedit/2013/03/28/55/100000000AEN20130328013500315F.HTML.}

To put such action in context, the Act was created and being promoted at the same time that the NIS was found to be committing political interference during elections in support of the current President.\footnote{125}{Choe Sang-Hun, South Korean Intelligence Officers Are Accused of Political Meddling, N.Y. TIMES, Apr. 19, 2013, at A8, available at http://www.nytimes.com/2013/04/19/world/asia/south-korean-intelligence-officers-are-accused-of-political-meddling.html.} In this case, the Seoul Metropolitan Police later found to have altered and destroyed evidence, as well as having national press conferences at unusual times to the benefit of the current President.\footnote{126}{Id.} This later resulted in large scale protests across the country that was rarely reported in national news.\footnote{127}{Stephen Borowiec, South Koreans Protest Alleged Election Interference, DEUTSCHE WELLE (Aug. 23, 2013), http://dw.de/p/19VEh.} Only a year later, the NIS was found to fabricate evidence related to a North Korean spy case, again for political
reasons. \(^{128}\) Citizen protests for NIS reform, culminated with President Park Geun-hye ordering the NIS to oversee its own reform.

While the Act attempts to combat cyber terrorism, to date attribution of major attacks against South Korean infrastructure has proven difficult. \(^{129}\) The majority of cases, such as the recent attack on Korean Hydro & Nuclear Power Company resulted in weak links back to North Korea. \(^{130}\) Without the help of China in such an investigation, all conclusions are conjecture that various organizations have framed as certainty. \(^{131}\)

The Act then does little prevent external attacks or improve the investigation of such attacks. It does, however, allow more control over national infrastructure and the legalization of private data access – for the NIS – that would otherwise be protected through procedure. \(^{132}\) This is similar to the United States and other countries, where the search for potential terrorists on national soil outweighs the privacy of the individual. \(^{133}\)

C. Growing Privacy Concerns

Incidents have led to increasing public criticism of the South Korean Government, such as how the government handled the Sewol Ferry sinking in 2014. \(^{134}\) Criticism of the government may be through online portals and chat programs. \(^{135}\) Many of the criticisms posted online in public and private conversations, although not usually illegal, were investigated by the Police and Prosecution services. \(^{136}\)

---


129. See Pauline C. Reich et al., *Cyber Warfare: A Review of Theories, Law, Policies, Actual Incidents - and the Dilemma of Anonymity*, 1 EUR. J. L. & TECH., no. 2, 2010, § 6.3, available at http://ejlt.org/article/view/40/58 (“There have been no reported arrests or prosecutions or reports of any military or other measures taken as a result of the attacks. One reason may be the problem of attribution of the exact source of the attacks.”).


131. *Id.*


133. *Id.*


This focus on negative criticism of the government through online channels eventually led many citizens to migrate from Korean-hosted chat service “Kakao Talk” to foreign chat services with a focus on encryption.\textsuperscript{137} After losing 1.5 million users Kakao Talk reversed its decision to monitor citizens private conversations.\textsuperscript{138}

Although South Korea has a number of strong laws concerning privacy protection, these are normally only applicable to Law Enforcement and Prosecution services, with Law Enforcement normally being held to high scrutiny.\textsuperscript{139} Organizations such as the NIS have special investigative powers under the premise of national security and use those powers online.\textsuperscript{140}

Government influence or control of critical infrastructure and major Korean software companies means on a practical level, Korean citizens have some privacy protection from Law Enforcement. But there is no effective privacy protection from other organizations. This situation is exacerbated in that Koreans are encouraged to use Korean-based software.\textsuperscript{141}

One example is the Korean-developed Hangul Word Processor.\textsuperscript{142} Although this software is used for word processing, the author has observed that the English version connects to an IP address registered to the Korea Internet & Security Agency (KISA). The reason for this is unclear, but in terms of privacy it is a potential concern for the large number of Koreans using nationally-developed, closed-source software.

\textbf{D. The Future of Privacy in Korea}

While the people of South Korea are concerned about privacy and security, there are special issues as to accountability and leadership. The leadership is still perceived as a noble class that the common people should not criticize. Where the government is not held fully accountable, there is a severe lack of

\textsuperscript{137} Dominique St. John, \textit{South Koreans Boycott Messaging App Kakao Talk En masse for Telegram, DEUTSCHE WELLE} (Aug. 8, 2014), \url{http://dw.de/p/1DRvz}.
\textsuperscript{140} Major Duties: Cyber Security, NIS, \url{http://eng.nis.go.kr/svc/major.do?method=content&cmid=11939} (last visited June 7, 2015).
\textsuperscript{141} See, e.g., Chico Harlan, \textit{South Korea Is Stuck with Internet Explorer for Online Shopping Because of Security Law}, \textit{WASH. POST.} (Nov. 5, 2013), \url{http://www.washingtonpost.com/world/asia_pacific/due-to-security-law-south-korea-is-stuck-with-internet-explorer-for-online-shopping/2013/11/03/fd2528a-3eff-11e3-b028-de922d7a3f47_story.html}.
\textsuperscript{142} See \textit{Hangul Word Processor}, \url{WIKIPEDIA}, \url{http://en.wikipedia.org/wiki/Hangul_character_set} (last visited June 7, 2015).
transparency. Through this lack of transparency, violation of privacy is likely commonplace, especially under the guise of national security. This is complicated by the ever-looming possibility of North Korean attacks on South Korea, either physically or online. This constant threat supports a ‘national security’ argument, which trades privacy for security.

The future of online privacy in Korea is promising. Korea is becoming more influenced by foreign companies and software, which will push some data out of the immediate grasp of the government. Further, younger Koreans are growing up relatively wealthy, relatively privileged, and without an understanding of the recent military dictatorship. Within a few short generations, these Koreans will demand more from the government in the form of transparency and privacy protections, especially for data. Korea will increasingly need to comply with international data privacy standards if it wants to compete in the international technology services market, and work with other countries on cyber crime investigation and prevention.

VIII. HONG KONG SAE, PEOPLES REPUBLIC OF CHINA

A. Roles of Hong Kong law enforcement agencies in surveillance

On January 26, 1841, the Far East Fleet of Great Britain landed in Hong Kong and raised the Union Flag. By May 1, 1844, the government gazette officially established the Colonial Police Force. By 1930, an Anti-Communist Squad had been set up within the Criminal Investigation Department of Hong Kong Police; it became the Special Branch and was central in maintaining Hong Kong’s colonial political order. The Special Branch monitored political

144. Id.
146. Id.
147. See, e.g., BBC, supra note 138.
150. TONY BANHAM, NOT THE SLIGHTEST CHANCE: THE DEFENCE OF HONG KONG 3 (1941).
activities and individuals and provided information leading to their detention, imprisonment or deportation.\footnote{153}{See \textit{Stanley S. Kwan \& Nicole Kwan, The Dragon and the Crown: Hong Kong Memoirs} 126 (2008).}

The Special Investigation Unit (\textquotedblleft SIU\textquotedblright) of the Special Crimes Division of the Hong Kong Police was created to deal with the \textquotedblleft Duffy Affair.\textquotedblright{} The arrest English solicitor for gross indecency with three boys but who was found to be him closely connected to a network of corruption.\footnote{154}{Attorney General v. John Richard Duffy, [1978] 85 H.K.L.R. (C.A.) (H.K.).} Although the SIU and the Special Branch were disbanded before the Chinese resumption of exercise of sovereignty over Hong Kong in 1997, political policing and monitoring doubtless continue under the new legal order.\footnote{155}{See Fu \& Cullen, \textit{supra} note 152, at 226.}

The \textit{Interception of Communications and Surveillance Ordinance} (\textquotedblleft ICSO\textquotedblright) came into force on August 9, 2006.\footnote{156}{Interception of Communications and Surveillance Ordinance, (2006) Cap. 589 (H.K.) \cite{http://www.legislation.gov.hk/blis_pdf.nsf/6799165D2EE3FA94825755E0033E532/DDA393C36B7FE4BA482575EF001FD1A4?OpenDocument&bt=0.} \textit{The ICSO applies to the activities of four law enforcement agencies: the Customs and Excise Department, the Hong Kong Police Force, the Immigration Department and the Independent Commission Against Corruption. The activities covered are the interception of communications and covert surveillance.}\footnote{157}{Kam C. Wong, Hong Kong Interception of Communications and Surveillance Ordinance: A Critical Assessment (June 25, 2007) (unpublished paper presented at the City University of Hong Kong School of Law conference entitled \textquotedblleft Hong Kong’s Basic Law: The First Ten Years and its Future\textquotedblright{}).} Covert surveillance is defined by section 2 of ICSO as:

(a) …any surveillance carried out with the use of any surveillance device for the purposes of a specific investigation or operation, if the surveillance --

(i) is carried out in circumstances where any person who is the subject of the surveillance is entitled to a reasonable expectation of privacy;

(ii) is carried out in a manner calculated to ensure that the person is unaware that the surveillance is or may be taking place; and

(iii) is likely to result in the obtaining of any private information about the person; but

(b) does not include --

(i) any spontaneous reaction to unforeseen events or circumstances; and
(ii) any such surveillance that constitutes interception under this Ordinance.\(^\text{159}\)

Interception is defined by section 2 of ICSO as:

(a) in relation to any communication, means the carrying out of any intercepting act in respect of that communication; or

(b) when appearing in a context with no specific reference to any communication, means the carrying out of any intercepting act in respect of any communication.\(^\text{160}\)

Communications covered are set out by section 2 of ICSO as:

(a) any communication transmitted by a postal service; or

(b) any communication transmitted by a telecommunications system;

(c) communication transmitted by a postal service includes a postal article.\(^\text{161}\)

Before law enforcement agencies carry out any interception or covert surveillance operations, they must obtain an authorization from either a panel judge appointed in accordance with ICSO or a designated senior law enforcement officer.\(^\text{162}\) The relevant authority for authorization depends on whether the application is for interception of communication, Type 1 surveillance or Type 2 surveillance, or an emergency; Type 1 surveillance requires judicial approval, Type 2 surveillance, as less intrusive, and emergency authorization require only executive/administrative approval.\(^\text{163}\)

Properly secured authorization or good faith performance under the ICSO provides immunity from any civil or criminal liability for actions performed by a person relating to surveillance or device retrieval.\(^\text{164}\)

The ICSO specifies two types of covert surveillance: Type 1 surveillance and Type 2 surveillance; the difference between the two types reflects the degrees of intrusiveness into privacy\(^\text{165}\). As a general rule, Type 2 surveillance involves the use of listening device or optical surveillance device and covers activities that would not necessarily require administrative approval in the United States.\(^\text{166}\) Any covert surveillance other than Type 2 surveillance is designated Type 1 surveillance.\(^\text{167}\) Further, any covert surveillance, even if Type 2 surveillance, requires special circumstances if it is likely that any information


\(^{160}\) Id.

\(^{161}\) Id.

\(^{162}\) Id. §§ 8, 14.

\(^{163}\) Id. §§ 3(1), 3(2) 8, 14, 20.

\(^{164}\) Id. § 65.

\(^{165}\) Id. § 2.

\(^{166}\) Id.

\(^{167}\) Id.
which may be subject to legal profession privilege or is related to journalistic materials will be obtained.\textsuperscript{168}

The ISCO especially provides for a Commissioner on Interception of Communications and Surveillance, who is a serving or former judge of the Court of First Instance or Court of Appeal, or a former permanent judge of the Court of Final Appeal.\textsuperscript{169} The Commissioner has the power to review all relevant records of law enforcement agencies, to require any public officer or other person to answer any question and provide information, and to require any officer to prepare a report on any case.\textsuperscript{170}

If a surveillance is not “covert surveillance,” ICSO does not apply.\textsuperscript{171} For example, is a 24-hour monitoring of Internet auction sites for any selling of infringing copies of copyrighted works “covert surveillance”? As a result of the monitoring, the IP address of the domain name and the server that hosts the domain, or even the IP address of a suspect’s email are obtained. This type of surveillance has been carried out by law enforcement agencies around the world.

Three criteria are set out in the definition of covert surveillance in section 2 of the ICSO. These criteria are that:

(i) any person who is the subject of the surveillance is entitled to a reasonable expectation of privacy;

(ii) the person is unaware that the surveillance is or may be taking place; and

(iii) likely to obtain any private information about the person.\textsuperscript{172}

The surveillance is covert when item (ii) is satisfied.\textsuperscript{173} On the other hand, the IP address of the domain name and the server that hosts the domain, or IP address of a suspect’s email are not private information in that they are generally available to the world for the functioning of the TCP/IP protocol for data transfer across the Internet. The subject under investigation would not have a reasonable expectation of privacy on the public auction sites. Therefore, no prescribed authorization would be required for such monitoring of auction sites. This calculus might change where various levels of protection or obfuscation are used, such as password-protected operations within the “Dark Web,” such as to require prior authorization for certain types of covert surveillance.

\textsuperscript{168} Id. §§ 31, 82.
\textsuperscript{169} Id. § 39.
\textsuperscript{170} Id. § 40.
\textsuperscript{171} Id. § 2.
\textsuperscript{172} Id.
\textsuperscript{173} Id.
IX. Conclusion

The globalization of networked instrumentation in so much of what people do will continue, with a growing data corpus linked to each of us. Computational systems and techniques of analyzing that data will continue to grow in predictive power. They offer significant benefits for safety and security as well as threats of greater abuse.

The wide and heterogeneous world of regulation, law and expectations is built on different cultures, traditions, histories and circumstances. Reconciling them all may be a task akin to the most difficult of trade agreements and peace treaties, as this throws together interests in personal autonomy, commercial power and national security.

These interests must be reconciled. The evolution and use of these systems would benefit from a shared ethical framework, at some level, that mitigates risks before the innocent suffer. This will be a difficult and fluid task that changes with the factual challenges people and their governments face. But it is an essential one as the power of such systems may shift further to those who control them, bringing new challenges for personal privacy and autonomy that impact who we are as a people.
MORE DATA MINING FOR MEDICAL MISREPRESENTATION?
ADMISSIBILITY OF STATISTICAL PROOF DERIVED FROM
PREDICTIVE METHODS OF DETECTING MEDICAL
REIMBURSEMENT FRAUD

Neil Issar∗

ABSTRACT

In recent years, the detection and prosecution of health care fraud has relied heavily on data mining and statistical models. Such models and methods of detection, while serving as powerful investigatory tools, nevertheless raise a number of legal concerns. They implicate scientific admissibility standards and courts’ historical disfavor of statistical methods of proof, while also raising concerns related to the reference class and blue bus problems. This paper will analyze the admissibility of statistical proof in cases alleging false recording of numeric codes for medical reimbursement. This is particularly relevant given that the U.S. government has mandated the replacement of ICD-9 code sets used by medical coders and billers to report health care diagnoses and procedures with ICD-10 codes, effective October 1, 2015 – a change that may increase physician liability under the False Claims Act.

I. INTRODUCTION

In recent years, the detection and prosecution of health care fraud has on occasion relied heavily on data mining and statistical models.1 Such methods of detection and statistical models, while offering powerful investigatory tools, nevertheless raise a number of legal concerns.2 For example, they implicate scientific admissibility standards established by the Supreme Court in Daubert v. Merrell Dow Pharmaceuticals (1993).3 They also implicate courts’ historical disfavor of statistical methods of proof, while raising concerns related to issues of propensity and the reference class and blue bus problems.4

This paper will analyze the admissibility of statistical proof in cases alleging false recording of numeric codes for medical reimbursement. This is particularly

∗ Vanderbilt University Law School, J.D. Candidate, Class of 2016. The author is grateful to Professor Edward K. Cheng for providing invaluable guidance and thought-provoking feedback for this paper.

1. See United States v. Chhibber, 741 F.3d 852, 854-55 (7th Cir. 2014). See also United States v. Mateos, 623 F.3d 1350, 1358 (11th Cir. 2010).
2. See Chhibber, 741 F.3d at 854.
relevant given that the U.S. Department of Health & Human Services (HHS) has mandated the replacement of ICD-9 code sets used by medical coders and billers to report health care diagnoses and procedures with ICD-10 codes—a change that may increase physician liability under the False Claims Act (FCA), 31 U.S.C. § 3729.5

Pursuant to the Health Insurance Portability and Accountability Act of 1996 (HIPAA)’s provisions on “Administrative Simplification,” the U.S. health care system requires providers to use the diagnostic coding system of the International Classification of Diseases and Related Health Problems (ICD).6 ICD-10 is the tenth revision of this system, and it utilizes codes of up to seven alphanumeric characters to identify disease categories, etiologies, affected body parts, illness severity, and additional factors to increase specificity and data precision.7

Already used by many parts of the health care industry across the developed world, ICD-10 features approximately seven times more reimbursement codes than the ones currently in use with ICD-9.8 This expansion was meant to address ICD-9’s inability to accommodate new codes for diagnoses and procedures that have been added to the health care repertoire of knowledge since the code set’s creation in 1979.9

Specifically, by diversifying the code set, providers should be able to better communicate to insurance companies the complexities of the treatments they deliver to patients.10 For health care providers, this more accurate—albeit, more complex—coding system will result in better data articulation, which could lower costs by more effectively evaluating complications and precisely tracking outcomes.11 ICD-10 could also help regulators and researchers gain a clearer view of the connections between the specific procedure performed, physician performance, and patient outcome or complications.12

However, the deadline for implementation of the new code set has been pushed back repeatedly as implementation involves installation and testing of new software while medical practices must simultaneously provide training for providers, staff members, and administrators.13 Practices will also need to

8. See id.
10. See id.
11. See id.
12. See id.
develop new practice policies and guidelines as well as update paperwork and forms.\textsuperscript{14} For convenience, practices may also create “crosswalks” or transition mappings that can convert frequently used ICD-9 codes to their ICD-10 equivalents, but there are problems regarding this aspect as well.\textsuperscript{15} The latest rescheduling of ICD-10’s mandatory implementation to October 1, 2015 marks the third such delay in the massive transition to the new coding system since it was first suggested in 2005.\textsuperscript{16}

More importantly, there is concern that ICD-10 codes will facilitate or increase the potentially devastating liability that health care providers face under the FCA and other fraud-related statutes and regulations.\textsuperscript{17} Critics have charged that health care providers often use coding to maximize billing opportunities, rather than to build the most accurate record possible.\textsuperscript{18} Despite the level of detail in ICD-10 codes, health care providers maintain some latitude in code assignment due to inter-provider subjectivity in diagnoses and procedures.\textsuperscript{19} This affords an opportunity for providers to scale-up services in an attempt to increase reimbursement—a practice known as “upcoding.”\textsuperscript{20} One study found that the practice of upcoding services provided to Medicare patients was prevalent and may account for as much as 15% of Medicare’s expenditures for general physician office visits, or over $2 billion per year.\textsuperscript{21} In addition, menus and lists built into new electronic health record software may encourage or incentivize physicians to charge for more services by suggesting items for which they can bill, auto- or pre-populating information from past patient encounters, and making it easy to click on boxes designed exclusively for reimbursement purposes.\textsuperscript{22}

Statistical evidence plays an important and expanding role in criminal investigations, prosecutions, and trials, and it may be a critical cog in predicting and prosecuting medical reimbursement fraud in light of the aforementioned changes and concerns under the ICD-10 coding system.\textsuperscript{23} For example, data

\begin{footnotesize}
\begin{itemize}
    \item 14. See id.
    \item 16. See Butler, supra note 13, at 24-28.
    \item 20. Id. at 224.
    \item 23. United States v. Chhibber, 741 F.3d 852, 854 (7th Cir. 2014).
\end{itemize}
\end{footnotesize}
mining algorithms for clustering medical treatment items, such as procedures or medical measurements, into several groups according to usage of different patients could detect if medical treatment items uncharacteristically shift from one cluster to another over short periods of time.\textsuperscript{24} Such statistical shifts may be used to label certain patients’ cases as fraud-suspicious for subsequent review.\textsuperscript{25} Similarly, pattern-mining techniques may be used to identify a set of structural patterns from clinical transactions and then identify aberrations or outliers from these patterns as potential cases of fraud.\textsuperscript{26} The unaddressed question—and the final focus of this paper—is whether statistical information from such predictive coding algorithms or models is admissible in court.

Part II of this paper will outline the parameters of medical coding and reimbursement in the health care industry while providing a background of the ICD system. Part II will also explain the development of the ICD’s tenth revision and how it differs from previous revisions; common methods of fraud that occur in the health care industry, with particular focus on upcoding; and how fraud may be detected. Part III will discuss the problems with and admissibility of statistical proof derived from predictive methods of detecting medical reimbursement fraud. Part IV concludes.

II. MEDICAL CODING & REIMBURSEMENT

The most common diagnosis and procedure code set used by health care providers to receive reimbursement has undergone various revisions, but the differences between the latest iterations are unprecedented. Health care providers depend on reimbursement from insurers and patients.\textsuperscript{27} To receive appropriate payment for health care services, a provider must communicate the underlying reasons, surrounding circumstances, and exact nature of services to a payer.\textsuperscript{28} This communication takes the form of coded information.\textsuperscript{29}

In its simplest form, medical coding is the “transformation of verbal descriptions into numbers.”\textsuperscript{30} Coding may also involve submitting attachments, which are “supplemental documents providing additional medical information to

\begin{itemize}
  \item \textsuperscript{24} See generally Patricia Cerrito & John C. Cerrito, \textit{Data and Text Mining the Electronic Medical Records to Improve Care and to Lower Costs}, http://www2.sas.com/proceedings/sugi31/077-31.pdf (last visited May 2, 2015).
  \item \textsuperscript{25} See Shunzhi Zhu et al., \textit{Health Care Fraud Detection Using Nonnegative Matrix Factorization}, 6 INT’L CONFERENCE ON COMPUTER SCI. & EDUC. 499 (2011).
  \item \textsuperscript{26} See Wan-Shiou Yang & San-Yih Hwang, \textit{A Process-mining Framework for the Detection of Healthcare Fraud and Abuse}, 31 EXPERT SYSS. WITH APPLICATIONS 56 (2006).
  \item \textsuperscript{28} Id. at 198.
  \item \textsuperscript{29} Id.
\end{itemize}
the claims processor that cannot be accommodated within the claim format.”

These attachments may include “Certificates of Medical Necessity (CMNs), discharge summaries and operative reports.”

But the coded information that a provider submits within a claim for reimbursement is still the most important component of the communication with a payer, and as such, must comply with standards outlined by statutes and health care regulations.

The most critical codes that appear on reimbursement claims are diagnosis codes and procedure codes, which together form “code sets.”

Sets of codes indicate the medical reasons for treatment and provide details about the treatment itself.

The most widely recognized diagnosis and procedure code set is the International Classification of Diseases (ICD), though it did not gain worldwide recognition until adoption of the code set’s sixth version (ICD-6) by the World Health Organization (WHO) in 1948.

Until that time, the code set’s revisions entailed minor changes. However, ICD-6 was more radical because it made it possible to record information from patient charts to compile morbidity statistics. ICD-6 also expanded the classification system to two volumes. Subsequent revisions were made in 1958 (ICD-7), 1968 (ICD-8), and 1979 (ICD-9).

In particular, ICD-9 was designed to describe the clinical picture in greater detail than ever before by specification of new clinical categories and extension of various coding rubrics. These changes resulted in the publication of an official U.S. variation dubbed the ICD-9 Clinical Modification (ICD-9-CM).

The latest version of the code set, ICD-10, was introduced in 1992.

A. ICD-9 vs. ICD-10

There are significant differences between the ninth and tenth versions of ICD, which raise concerns about difficulties in transition that may contribute to coding errors and health care fraud. During the creation of ICD-9, the WHO
realized that more extensive classification changes would need to be implemented in the near future.\textsuperscript{43} As a result, development of the tenth revision of ICD was initiated even before the ninth version was completed.\textsuperscript{44} In the United States, the National Center for Health Statistics (NCHS) is responsible for updating the ICD, and the organization created a version known as the International Classification of Diseases, Tenth Revision, Clinical Modification (ICD-10-CM) after incorporating public suggestions and field-test results.\textsuperscript{45} However, concerns arose given the dramatic changes between ICD-9 and ICD-10.\textsuperscript{46}

ICD-9 diagnosis codes are divided by body system.\textsuperscript{47} As medical knowledge grew and classifications expanded over the years, the more complex body systems ran out of codes.\textsuperscript{48} The lack of codes within their appropriate chapters resulted in new codes being assigned in chapters of other body systems.\textsuperscript{49} This forced rearrangement of codes made locating the correct code more complicated for health care providers inexperienced in medical coding.\textsuperscript{50} This, in part, resulted in demands for a new classification system that was “flexible enough to quickly incorporate emerging diagnoses and procedures” yet “exact enough to identify diagnoses and procedures precisely.”\textsuperscript{51} ICD-10-CM is supposed to fulfill this need for flexibility and precision.

The codes in ICD-10 are alphanumeric while codes in ICD-9 are simply numeric.\textsuperscript{52} Each code in ICD-10 starts with a letter (i.e., A–Z), followed by two numeric digits, a decimal, and one to four digits or letters (e.g., primary generalized osteoarthritis is coded as M15.0).\textsuperscript{53} In contrast, codes in ICD-9 begin with three digit numbers (i.e., 001–999), that are followed by a decimal and up to two digits (e.g., primary generalized osteoarthritis was coded as 715.00).\textsuperscript{54}

In addition, while both ICD-9 and ICD-10 maintain the diagnosis-procedure code dichotomy, there is a staggering difference in the absolute number of codes of each type. ICD-9 contains 14,567 diagnosis codes while ICD-10 contains

\textsuperscript{43} Maxim Topaz et al., ICD-9 to ICD-10: Evolution, Revolution, and Current Debates in the United States, 10 Persp. Health Info. MGMT. 1, 1 (2013).
\textsuperscript{44} Id.
\textsuperscript{45} See id. at 2.
\textsuperscript{46} Christopher G. Chute et al., There Are Important Reasons For Delaying Implementation Of The New ICD-10 Coding System, 31 Health Aff. 836, 838-41 (2012).
\textsuperscript{48} Id.
\textsuperscript{49} Id. For example, ICD-10 has 21 categories of disease compared to 19 categories in ICD-9-CM, and the category of “diseases of the nervous system and sense organs” in ICD-9-CM is divided into three categories in ICD-10, including diseases of the nervous system, diseases of the eye and adnexa, and diseases of the ear and mastoid process. Quan et al., supra note 36, at 1425.
\textsuperscript{50} Sutyak, supra note 47, at 5.
\textsuperscript{51} Id. at 5.
\textsuperscript{52} Quan et al., supra note 14, at 1425.
\textsuperscript{53} Id.
\textsuperscript{54} Id.
69,832 diagnosis codes. 55 Similarly, in ICD-9 there are 3,878 procedure codes while ICD-10 contains 71,920 procedure codes. 56 The transition to ICD-10 requires that all health care providers, including physicians and hospitals, use the diagnosis portion of ICD-10. 57 However, the procedure portion of ICD-10 is only used by hospitals for reporting inpatient procedures. 58

Instead of creating complexity and difficulty of use, the increased number of codes and specificity in ICD-10 should theoretically make coding simpler. 59 The challenge of accurate coding allegedly resulted from the lack of detail in ICD-9 codes, since ambiguity can result in disagreements about what certain codes mean and when they should be used. 60 Accordingly, ICD-10 sought to increase specificity to decrease the claims adjudication costs associated with requests for clarifications or additional information and rejected claims, which should result in fewer delays and significant administrative simplification for both providers and payers. 61

The increase in the total number of ICD-10 diagnosis codes, in particular, can largely be attributed to a systematic expansion in the level of anatomic specificity. 62 It has been argued that the difference in the number of codes is relatively small for most physician specialties and that most codes contain the same level of detail familiar to users of the well-established ICD-9 code set. 63 In addition, some of the new coding terminology merely replaced terms that were deemed obsolete in the medical literature. 64

However, there are examples where the level of detail in ICD-10 diagnosis codes increases dramatically. 65 For example, ICD-9 code 996.1 refers to “Mechanical complication of other vascular device, implant and graft.” 66 This code and its associated diagnosis contains no information on the type of surgical complication (i.e., breakdown, displacement, leakage, etc.) or the type of device, implant, or graft (e.g., aortic graft, dialysis catheter, arteriovenous shunt, counterpulsation balloon, etc.). 67 In ICD-10, precise detail about the type of surgical

56. Id.
57. Id.
58. Id.
59. Id. at 2.
60. See id.
61. Id. at 2.
62. Id. at 3.
63. See id.
64. See id. (For example, the ICD-9 separation of asthma into extrinsic and intrinsic asthma is not maintained in ICD-10). See also Stephanie Romanent-Manent et al., Allergic vs Nonallergic Asthma: What Makes the Difference?, 57 ALLERGY 607, 607 (2002).
67. See Averill & Butler, supra note 55, at 3.
complication and the device, implant, or graft used is provided. While this results in one ICD-9 code being expanded into over 150 possible ICD-10 codes, it has been argued that this level of detail is necessary given the health care system’s greater emphasis on linking quality, payment, and value-based purchasing after statutory reform measures enacted over the past few years.

By enabling more detailed patient history coding, ICD-10 may be able to better coordinate a patient’s care across providers and over time. ICD-10 may also improve quality measurement and reporting, facilitate the detection and prevention of fraud, waste, and abuse, and lead to greater accuracy of reimbursement for medical services. Through these improvements, the NCHS aims to augment public health surveillance, national quality reporting, and overall health care research and data analysis. As such, ICD-10 represents a significant change that impacts the entire health care community. Accordingly, considerable resources have been invested toward the transition to ICD-10, and the Centers for Medicare and Medicaid Services (CMS) has implemented a comprehensive testing approach, including end-to-end testing in 2015, to help ensure providers are ready.

However, many have complained that the government is distorting the reality regarding the usefulness and improvements of ICD-10. A Canadian study analyzed administrative hospital discharge data using both ICD-9-CM and ICD-10-CM code sets and concluded that the “functional capacity of ICD-10-CM was not materially different than that of ICD-9-CM.” This suggests that ICD-10 was not practically better than ICD-9 for coding clinical data.

There have also been claims that ICD-10 increases proliferation of codes to an absurd degree. For example, ICD-9 contained one code for angioplasty, while...

---

68. Id. For example, under ICD-10-CM, code categories T80 to T88 include codes for “Complications of surgical and medical care, not elsewhere classified.” But each group is reserved for specific types of devices, implants, or grafts. T82, for example refers to “Complications of cardiac and vascular prosthetic devices, implants and grafts,” while T83 refers to “Complications of genitourinary prosthetic devices, implants and grafts.” The next digit in the ICD-10-CM code specifies the exact type of device, with subsequent digits and letters providing greater detail about the type of complication and encounter. Thus, T82.01XA refers specifically to “Mechanical complication (breakdown) of heart valve prosthesis on initial encounter.” All of this detail would be missed under ICD-9 coding.

69. See id.


71. Id.

72. See id.

73. Id.


75. Id.
ICD-10 contains over 850. Similarly, ICD-10 contains 195 codes for suturing an artery and 312 codes that involve animals. Moreover, of the 140,000 new codes that will be available, some appear either unnecessarily specific or simply unnecessary: W61.42 (Struck by turkey), which is distinct from W61.43 (Pecked by turkey); S45.911 (Laceration of unspecified blood vessel at shoulder and upper arm level, right arm); S91.232 (Puncture wound without foreign body of left great toe with damage to nail); R46.0 (Very low level of personal hygiene); T71.233 (Asphyxiation due to being trapped in a (discarded) refrigerator, assault); Y92.65 (Oil rig as the place of occurrence of the external cause); Y92.72 (Chicken coop as the place of occurrence of the external cause); T43.612 (Poisoning by caffeine, intentional self-harm); and V04.09 (Pedestrian on snow skis injured in collision with heavy transport vehicle or bus in non-traffic accident).

While specificity and greater coverage of medical scenarios may indeed be helpful for coding and reimbursement purposes, it appears ICD-10 has taken this to an extreme. There is an as of yet undefined threshold of detail that, when crossed, shifts medical coding from invaluable to indecipherable. Since there are legitimate concerns that ICD-10 crosses such a threshold, the impending transition may result in increased coding errors by both health care providers and professional coders, and it may increase opportunities for health care fraud.

B. Complications in Transition

The transition to ICD-10 will be complicated by insufficient coding training, a lack of unanimity in coding among both health care providers and professional coders, and an initial lack of productivity. Despite the critical importance of coding and billing, physicians spend little time teaching or learning about billing either during residency training or after starting their own practices. Although resident physicians spend three or more years during residency, and often additional years during fellowship, acquiring clinical decision making and technical skills, little to none of the training focuses on medical coding.

While lack of resident and fellow education in ICD coding is common among many medical disciplines, scope of practice may mitigate this problem.

77. Id.
78. Id.
80. See Scott D. Lifchez et al., Ethical and Educational Considerations in Coding Hand Surgeries, 39 J. HAND. SURG. AM. 1370, 1370 (2014).
81. See id. at 1373.
82. See id. at 1375.
83. Id.
Providers with a highly focused practice, such as surgeons with fellowship specialization in private practice, may need only a few codes to describe the vast majority of procedures they perform. Nonetheless, the additional code choices associated with ICD-10 will increase coding difficulties. Even a hand surgeon, for example, will now require designation of the specific digit involved, initial versus subsequent visit, and presence or absence of complications—details that were not encompassed by most ICD-9 codes.

In addition, a large body of studies document that physicians are frequently inaccurate in their coding, though accuracy has improved over time. Many surgeons rely on professional coders to assist in the coding process, but the aforementioned problems associated with physician coding are exacerbated as there is disagreement even among professional coders about how a visit, diagnosis, or treatment should be coded. Inaccuracies in ICD-10 coding threaten timely reimbursement for services and exposes providers to civil or even criminal penalties. Coding inaccuracy may simply be due to a lack of knowledge of coding rules or practices, but it may also be attributable to

84. Id.
85. See id.
86. See, e.g., Elaine M. Burns et al., Systematic Review of Discharge Coding Accuracy, 34 J. PUB. HEALTH 138, 141 (2012) (analyzing 32 studies investigating the accuracy of hospital episode data and coding, and finding an overall median accuracy of 83% with procedure accuracy (84.2%) found to be higher than primary diagnosis coding (80.3%) and considerable variation in accuracy rates between studies (50.5-97.8%)); John C. Hwang et al., Representation of Ophthalmology Concepts by Electronic Systems: Intercoder Agreement among Physicians Using Controlled Terminologies, 113 OPHTHALMOLOGY 511 (2006) (finding complete CPT intercoder agreement on approximately 55% of ophthalmology cases); Mitchell S. King et al., Accuracy of CPT Evaluation and Management Coding by Family Physicians, 14 J. AM. BOARD FAM. PRAC. 184, 187 (2001) (finding in a survey of 600 family physicians that the physicians agreed with expert billing coders 52% of the time); Thomas J. Zubet al., Variability in Code Selection Using the 1995 and 1998 HCFA Documentation Guidelines for Office Services, 49 J. FAM. PRACT. 642 (2000) (finding that only 29.2% of physicians agreed with a faculty family practice physician on visit codes, and that physicians agreed with professional coders only 51.7% of the time); George E. Kikano et al., Evaluation and Management Services: A Comparison of Medical Record Documentation with Actual Billing in Community Family Practice, 9 ARCHIVE FAM. MED. 68, 70 (2000) (finding 57% concordance between family physician CPT billing codes and codes based on medical record review from expert encoders); Chao et al., Billing for Physician Services: a Comparison of Actual Billing with CPT Codes Assigned by Direct Observation, 47 J. FAM. PRACT. 28 (1998) (finding 55% concordance between the billing codes entered by 138 family physicians and trained expert encoders). See also Anil Kumar Pillai & Andrew R.L. Medford, Greater Physician Involvement Improves Coding Outcomes in Endobronchial Ultrasound-Guided Transbronchial Needle Aspiration Procedures, 85 RESPIRATION 417, 419-20 (2013) (finding that physician coding errors could be improved by greater physician engagement with coders and by cross-checking against a procedural database).
87. See, e.g., Mitchell S. King et al., Expert Agreement in Current Procedural Terminology Evaluation and Management Coding, 162 ARCHIVE INTERNAL MED. 316 (2002) (finding 57% agreement among 300 certified professional coding specialists on six hypothetical medical cases, with the level of agreement for individual cases ranging from 50-71%); Lifchez et al., supra note 80, at 1375 (finding a wide range in practice regarding how to code relatively common procedures, with no uniformity in agreement for coding of six hypothetical cases).
88. Lifchez et al., supra note 80, at 1375.
practices intended to increase reimbursement for individual patients or procedures.\textsuperscript{89}

Other complications related to the ICD-10 transition include an initial loss of productivity. When Canada transitioned to its ICD-10 iteration in the early 2000s, there was a 52\% loss of productivity following the implementation of the new code set.\textsuperscript{90} It took three to six months after implementation to identify any significant improvements in productivity.\textsuperscript{91} In addition, another study reviewed over four thousand charts for patients admitted over a six-month period at four teaching hospitals in Alberta, Canada, to assess the conformity between ICD-9-CM and ICD-10 coding as well as the accuracy of each code set in matching chart data.\textsuperscript{92} The study found that ICD-10 data had significantly higher sensitivity for one condition and lower sensitivity for seven conditions relative to ICD-9-CM data.\textsuperscript{93} It is possible that lower ICD-10 sensitivity was attributable to coders being in the early portion of an ICD-10 learning curve.\textsuperscript{94} It is also possible that coders who recoded charts in ICD-9-CM simply performed better than regular coders who coded ICD-10.\textsuperscript{95} Regardless of causation, the study made it clear that the transition to ICD-10 did not significantly improve the quality of administrative data relative to ICD-9-CM.\textsuperscript{96}

Conversely, one study hypothesized that ICD-10-CM could be comparatively more flexible because of its capacity to incorporate new codes over time.\textsuperscript{97} The study analyzed over 2700 diagnosis codes and found that 26\% of all pediatric ICD-9-CM codes and 21\% of pediatric patient visits were associated with “convoluted” codes—codes with complex mappings that made the ICD-9 to ICD-10 transition difficult.\textsuperscript{98} Over 600 convoluted codes were analyzed for accuracy and nearly 40\% were categorized as information loss, inconsistent, or overlapping.\textsuperscript{99} Convoluted codes of this sort, many of which require non-intuitive details to be understood, have the potential to cause inaccuracies during the ICD-

\textsuperscript{89} See id.
\textsuperscript{91} Rahmathulla et al., supra note 79, at S189.
\textsuperscript{92} Quan et al., supra note 36, at 1427.
\textsuperscript{93} Id. at 1431-35 (“Sensitivity was “calculated to measure the extent of recording the presence of conditions in administrative data when these were present in the chart review data.”).
\textsuperscript{94} Id. at 1435.
\textsuperscript{95} Id. at 1436.
\textsuperscript{96} Id.
\textsuperscript{97} Richard Caskey et al., \textit{The Transition to ICD-10-CM: Challenges for Pediatric Practice}, 134 PEDIATRICS 1, 2 (2014).
\textsuperscript{98} Id. at 3.
\textsuperscript{99} Id. (“Information loss” was used when the transition obscures a clinically important diagnostic distinction, resulting in a potential loss of relevant clinical detail. “Overlapping category” was used when the transition results in a distinction without a clinically relevant difference or could result in confusion for appropriate code assignment. “Inconsistent” was used when ICD-10-CM codes were clinically different than the ICD-9-CM codes to which they mapped.)
This, in turn, could lead to billing errors, errors in surveillance, and inaccurate administrative data, all of which could have detrimental financial effects.\textsuperscript{101}

To help facilitate care and to ameliorate some of the transition difficulties outlined above, the CMS has endorsed two types of mappings to transition between ICD-9 and ICD-10: general equivalence mappings (GEMs) (for both ICD-9 to ICD-10 and ICD-10 back to ICD-9) and reimbursement maps (for ICD-10 to ICD-9 only).\textsuperscript{102} GEMs establish links among codes that are generally equivalent in each code set.\textsuperscript{103} In contrast, reimbursement maps were created after GEMs and are more specific as they identify top candidate mappings from within preexisting GEMs.\textsuperscript{104}

However, there are challenges inherent even in linking across the two code sets. For example, there are 255 instances where a single ICD-9 code can map to more than 50 ICD-10 codes, and 119 instances where a single ICD-9 code can map to more than 100 ICD-10 codes.\textsuperscript{105} In addition, some GEMs maps of ICD-9 to ICD-10 are not specific, as there are 7,239 instances in the mappings for diseases where a single ICD-10 code can map to more than one ICD-9 code, and 7,241 instances of procedure mappings where the same problem occurs.\textsuperscript{106} Thus, despite the proposed ease of use and advantages of ICD-10, it is clear that there remain many problems in transitioning to it from the well-established ICD-9. The existence of these problems buttress the arguments of those pushing for another delay in the mandatory implementation date.\textsuperscript{107}

Health care providers and payers in the United States were initially scheduled to adopt ICD-10-CM in 2008, but the CMS pushed back the deadline to October 2013.\textsuperscript{108} The reason was that the conversion required health care providers and payers to adapt their information systems to accommodate the aforementioned increase in new diagnostic and payment codes.\textsuperscript{109} After further lobbying by the American Medical Association (AMA), American Academy of Orthopaedic Surgeons (AAOS), and other organizations, the CMS postponed implementation until October 2014, and then pushed it further ahead to October 2015.\textsuperscript{110}

\begin{thebibliography}{99}
\bibitem{100} See id. at 4.
\bibitem{101} Id.
\bibitem{102} Manchikanti et al., supra note 38, at E418.
\bibitem{103} Id.
\bibitem{104} Id. at E418-20.
\bibitem{105} Id. at E420 (citing John Wollman, \textit{ICD-10: A master data challenge}, 32 \textit{Health Mgmt. Tech.} 16 (2011)).
\bibitem{106} Id. (citing Wollman, supra note 105, at 16).
\bibitem{108} Chute et al., supra note 74, at 836–37.
\bibitem{109} Id.
\bibitem{110} M. Bradford Henley, \textit{ICD 10: What Orthopedic Surgeons Should Know, How It Will Affect Them, and the Cost of Implementation?}, 21 SPORTS MED. ARTHROSCOPY 142, 142 (2013). The final
Various studies indicate that the delay in implementation may have been warranted. For example, two surveys of physicians in 2014 found that 50% of respondents indicated that ICD-10 will cause severe administrative problems in their practices, while 67–75% felt that ICD-10 would unnecessarily complicate coding. Correspondingly, less than 10% of physician practices were prepared for the ICD-10 conversion, and this lack of provider readiness was a major reason Congress pushed back the 2014 deadline. When asked to rate their practice’s “overall readiness level for ICD-10 implementation,” only 9.4% of respondents reported having made “significant progress,” whereas 79% were “somewhat ready” or had not even started implementation. None reported having completed preparations for the transition. Similarly, a 2014 ICD-10 Industry Readiness Survey indicated that only approximately 50% of health care providers had assessed the impact of ICD-10 on their practices, and this number had not increased from the 2013 survey that asked about assessing the same impact. In addition, only 35% of providers had begun external testing even though 60% of respondents to the 2013 survey indicated that they planned to begin testing by the middle of 2014.

Some have argued that forgoing the currently scheduled transition to ICD-10 would translate into a loss of billions of dollars for the U.S. health care industry. Many of the largest health care systems have already spent considerable resources to meet the implementation deadline, and the government has estimated the cost of a one-year delay to range from $1.1 billion to $6.8 billion. In addition, retraining personnel and reconfiguring systems numerous times is not only costly but also time-consuming, which can further delay the implementation process. Moreover, the delay in implementation has created uncertainty for both the health care providers and the patients, as they have to adapt to the new coding system at a later stage.
times in anticipation of the transition is unnecessarily driving up costs. Moreover, extending the delay could render current ICD-10 system updates and releases obsolete, diminishing investments stakeholders have already made to prepare for transition.

Despite multiple delays in the statutorily mandated transition date for ICD-10, concerns remain regarding inadequate training in coding, a lack of unanimity in coding between both health care providers and professional coders, and a possible decrease in post-implementation productivity. This may contribute to increased coding errors by both health care providers and professional coders, and it may increase opportunities for health care fraud, thereby affecting physician liability under the False Claims Act (FCA).

C. Health Care Fraud and Upcoding

The frequency and extent of health care fraud has grown dramatically over the past two decades, despite a corresponding intensity of efforts to combat it, and coding is increasingly a key aspect in many fraud cases. In 1993, the chief of the criminal division in the Office of the New York State Special Prosecutor for Medicaid Fraud Control testified before the House of Representatives to discuss the problem of Medicaid fraud. He estimated that 5–20% of Medicaid expenditures were being lost to fraud and abuse on an annual basis, and he characterized the problem as a “feeding frenzy” in which profiteers were exploiting “great loophole[s] in the Medicaid system.”

Two years later, the Chairman of the U.S. Senate Special Committee on Aging addressed the Senate on the same issue, and further clarified that committing health care fraud had become “appallingly easy” due to the “size,
complexity, and splintering” of the system.\textsuperscript{124} He, too, described the problem as a “feeding frenzy”—one in which “taxpayers are paying the tab for their feast.”\textsuperscript{125} Despite these warnings about the issue, the problem of health care fraud has continued unabated.\textsuperscript{126} Today, coding presents an additional concern to payers and the public, and it has been revealed as a prominent tool in many fraud cases.

The CMS exacts monetary penalties for coding fraud under HIPAA, and the government recovered over $400 million dollars in 2012 alone for disallowed services and restitution/damages for fraudulently billed services.\textsuperscript{127} In addition, the FCA is a federal statute that creates civil liability for entities that falsely or fraudulently contract with the government to provide or receive services or goods in exchange for funds.\textsuperscript{128} With the growth of Medicare and Medicaid funding for health care services, there has been a corresponding increase of false claims and FCA cases.\textsuperscript{129}

One way by which coding has become implicated in fraud cases is “upcoding”: the practice of maximizing reimbursement by exaggerating the severity of certain cases, diagnoses, or procedures when coding.\textsuperscript{130} Upcoding has

\begin{thebibliography}{99}

\bibitem{125} Id.

\bibitem{126} For example, approximately 9% (corresponding to $47.9 billion) of the government’s Medicare expenditures was lost due to fraud in 2010. See Qi Liu & Miklos Vasarhelyi, Healthcare fraud detection: A survey and a clustering model incorporating Geo-location information, 29TH WORLD CONTINUOUS AUDITING AND REPORTING SYMPOSIUM, at 1 (2013). Proportionately, this is comparable to Thomas Staffa’s estimate of the extent of financial loss suffered by Medicaid due to fraud in 1993. See Statement of Thomas F. Staffa, supra note 122. Some estimates have placed overall health care fraud losses to be in excess of $100 billion. See James D. Byrd et al., Health care Fraud: An Introduction to a Major Cost Issue, 14 J. ACCT. ETHICS & PUB. POL’Y, 521, 522 (2013). See also Medicare Fraud: A $60 Billion Crime, CBS NEWS (Sep. 5, 2010), http://www.cbsnews.com/8301-18560_162-5414390.html (“In fact, Medicare fraud - estimated now to total about $60 billion a year - has become one of, if not the most profitable, crimes in America.”); Walecia Konrad, As Medicare Fraud Evolves, Vigilance Is Required, N.Y. TIMES (Sep. 11, 2012), http://www.nytimes.com/2012/09/12/business/retirement-special/medicare-fraud-victimizes-patients-and-taxpayers.html (noting that CMS estimates that Medicare and Medicaid made more than $65 billion in improper federal payments in 2010 and as much as ninety-eight billion dollars in 2011).

\bibitem{127} Lifchez et al., supra note 80, at 1370.


\bibitem{129} See id. at 166; LeClairRyan, Feds Use Tougher Tactics to Fight Healthcare Fraud, PR NEWSWIRE, (Sept. 7, 2012), http://www.prnewswire.com/news-releases/feds-use-tougher-tactics-to-fight-healthcare-fraud-168904666.html (noting an increase in recovery for both civil and criminal healthcare fraud cases).

\bibitem{130} PAUL LANDAIS ET AL., MEDICAL INFORMATICS, E-HEALTH: FUNDAMENTALS AND APPLICATIONS 193 (Alain Venot et al. eds., 2014) (The concept of upcoding was first introduced by Dr. Donald Simborg in 1981 as a new type of “disease” in U.S. hospitals.). See Donald W. Simborg, DRG Creep – A New Hospital-Acquired Disease, 304 NEW ENG. J. MED. 1602 (1981).
\end{thebibliography}
also been defined as differences in coding practices across reimbursement plans that would lead to two plans generating distinct risk scores for the same individual.\textsuperscript{131} Some diagnoses have specifically been identified as associated with higher resource consumption, and are consequently termed “complications” in the coding lexicon.\textsuperscript{132} In many reimbursement systems, the presence of a complication will result in higher reimbursement; this is the primary mechanism via which upcoding can occur,\textsuperscript{133} since making patients look sicker on paper yields higher payments.\textsuperscript{134} Upcoding is ubiquitous among hospitals paid under diagnosis-related group (DRG) or capitated Medicare Advantage (MA) plans, which use it to extract overpayments of $30 billion annually.\textsuperscript{135}

There are also ways that insurers, rather than (or in combination with) health care providers, can influence medical coding, risk scoring, and upcoding. Insurers can contract with physician groups such that the payment to the group is a fraction of the risk-adjusted payment that the insurer itself receives from the regulator; this incentivizes the contracting physicians to maximize codes associated with higher reimbursement.\textsuperscript{136} Insurers may also choose to selectively contract with providers who code more meticulously or aggressively.\textsuperscript{137}

In addition, insurers can act subtly by dedicating more resources to ensure careful and meticulous coding of every eligible diagnosis.\textsuperscript{138} For example, insurers may influence coding during the medical exam itself by providing software to physicians that auto- or pre-populate electronic health records with information from the patient’s prior visits.\textsuperscript{139} This increases the probability that old diagnoses are erroneously retained in the note.\textsuperscript{140} Another strategy is to require patients to come in each year for an “evaluation and management visit,” which is inexpensive to the insurer, but during which codes can be added that otherwise would have gone undiscovered.\textsuperscript{141} At the extreme, health care

\begin{itemize}
\item \textsuperscript{131} Michael Geruso & Timothy Layton, \textit{Upcoding or Selection? Evidence from Medicare on Squishy Risk Adjustment}, 25TH ANN. HEALTH ECON. CONF. 7 (Oct. 16, 2014).
\item \textsuperscript{132} Landes et al., \textit{ supra} note 130, at 195.
\item \textsuperscript{133} See \textit{id}.
\item \textsuperscript{134} David U. Himmelstein & Steffie Woolhandler, \textit{Global Amnesia: Embracing Fee-For-Non-Service – Again}, 29 J. GEN. INTERNAL MED. 693, 693–94 (2014).
\item \textsuperscript{135} Id. at 694 (citing Jason Brown et al., \textit{How does risk selection respond to risk adjustment? Evidence from the Medicare Advantage program} (Nat’l Bureau of Econ. Research, Working Paper No 16977, 2011)). \textit{See also} Timothy J. Layton, Risk Selection and Risk Adjustment in Competitive Health Insurance Markets (2014) (unpublished Ph. D. dissertation, Boston University) (on file with author) (finding that risk scores in Medicare Advantage (MA) plans are approximately 4% higher than they would have been in Fee-for-Service (FFS) Medicare plans for the same beneficiary).
\item \textsuperscript{136} See Geruso & Layton, \textit{ supra} note 131, at 9.
\item \textsuperscript{137} See \textit{id}.
\item \textsuperscript{138} See Layton, \textit{ supra} note 135, at 100.
\item \textsuperscript{139} See Geruso & Layton, \textit{ supra} note 131, at 9.
\item \textsuperscript{140} See \textit{id}.
\item \textsuperscript{141} Layton, \textit{ supra} note 135, at 100.
\end{itemize}
providers and insurers can commit outright fraud by adding or changing codes in patients’ records without any medical justification.  

Overall, the transition to ICD-10 could increase physician liability under the FCA since (1) the increase in codes, difficulties in coding, and problems with transition maps such as GEMs will increase coding errors; (2) greater specificity may make it easier for plaintiffs to demonstrate that such coding errors were done “knowingly,” thereby satisfying the FCA’s sciener requirement; and (3) lack of precedent for ICD-10 coding submissions will provide greater opportunities for fraudulent forms of coding, such as upcoding, by health care providers and insurers alike.  

D. Methods of Detection

It is clear that the size of the health care sector and the enormous volume of money involved make it an attractive fraud target. Consequently, effective fraud detection is important for controlling rising health care costs. However, this has been complicated by the increasing number of records in medical databases, and, now, the complexity of the codes associated with each record—complexity that will increase exponentially with the transition to ICD-10. Thus, data mining has progressively played an important role in fraud detection since it can uncover and extract specific information from very large quantities of data.

142. See, e.g., United States v. Janke, No. 09-14044-CIV, 2009 WL 2525073, at *1, 3 (S.D. Fla. Feb. 10, 2009) (the defendant physician and his wife were accused of personally directing “data sweeps” of thousands of beneficiary medical files to collect additional, unjustified diagnoses to inflate Medicare payments; hiring unlicensed physicians to conduct these sweeps; urging these physicians to seek out any evidence of major medical diagnoses to inflate fraudulent Medicare claims; knowingly taking part in meetings and correspondence discussing a computer system that reported false data to the CMS; receiving independent confirmation from two potential buyers and from their own hired expert that their risk adjustment submissions contained false claims, but failing to report this information to CMS; warning their employees to not cooperate with official government investigations; and depositing over $12,000,000 in Medicare payments into their personal bank account). The Janke case resulted in a settlement of $22.6 million to resolve allegations that the defendants caused Medicare to pay inflated amounts based upon the submission of false diagnosis codes. See Press Release, Dep’t of Justice – Office of Pub. Affairs, Florida-based Medicare Advantage Plan Owners & Primary Care Provider Agree to Pay $22.6 Million to Settle Claims of Falsifying Diagnoses (Nov. 24, 2010), available at http://www.justice.gov/opa/pr/florida-based-medicare-advantage-plan-owners-primary-care-provider-agree-pay-226-million.


145. See Liu & Varsarhelyi, supra note 126.

146. See supra, Part II.A.

Data mining has been defined both as a process of identifying interesting patterns in databases that can then be used in decision making, and as a process that uses statistical, mathematical, artificial intelligence, and machine learning techniques to extract and identify useful information and subsequently gain knowledge from a large database. Under both definitions, the objective of data mining is to obtain useful, non-explicit information from data stored in large repositories. An important advantage of data mining is that it can be used to identify new forms of fraud before they can be detected by human experts. For this reason, fraud detection has become one of the best established applications of data mining by both industry and the government.

Data mining methods of fraud detection can be classified as supervised, unsupervised, or a combination of both (referred to as hybrid or “semi-supervised” methods). Supervised methods involve data mining algorithms that have been “trained” by the input of transactions that have been previously identified or “labeled” as either fraudulent or non-fraudulent by human experts. The algorithms then identify profiles of health care providers’ transactions that share certain features or levels of similarity with the transactions previously labeled as fraudulent. Examples of supervised data mining methods include, inter alia, neural networks, logistic regression models, the naïve Bayesian method, and decision trees. Conversely, unsupervised methods do not entail any previous labeling of data, while semi-supervised methods use some data that is labeled and some unlabeled data that is evaluated during the processing of transactions. Semi-supervised and unsupervised methods can

149. Efraim Turban et al., Decision Support and Business Intelligence Systems (Bob Horan et al., eds., 8th ed. 2010).
152. Clifton Phua et al., A Comprehensive Survey of Data Mining-Based Fraud Detection Research, ARTIFICIAL INTELLIGENCE REP. 1 (2010).
155. See Aral et al., supra note 153, at 38.
157. See Copeland et al., supra note 154, at 53.
identify outliers and “learn” fraud patterns from data, allowing them to identify new types of fraud that were not previously documented.\textsuperscript{158}

Supervised methods can be used to calculate, among other things, the probability that a patient episode is coded incorrectly.\textsuperscript{159} Similarly, Bayesian co-clustering modeling may be used to identify possible “conspiracy fraud”—fraud committed by collusion between two or more parties.\textsuperscript{160} Co-clustering allows detection of unusual provider-beneficiary pairings and identification of atypical associations among provider and beneficiary clusters.\textsuperscript{161} In comparison to co-clustering, human evaluators and traditional statistical analyses are far less effective in describing and capturing the relationships that connect providers and beneficiaries in order to identify suspicious monetary charges associated with certain provider-beneficiary pairs for further investigation.\textsuperscript{162} There is also a trend towards combining several supervised methods to improve results.\textsuperscript{163}

Training of supervised models has advanced to the point where algorithms can isolate or ignore “noise” (caused by human subjectivity or bias in labeling training datasets), handle missing values, and differentiate irrelevant attributes.\textsuperscript{164} However, because past data from which the supervised models are trained can be limited in quantity and scope, supervised approaches are correspondingly limited in their applicability.\textsuperscript{165} This limitation has spurred development of more advanced unsupervised methods of fraud detection. The most common method involves identifying outliers from claim amounts or utilization rates to “flag” for secondary, individualized investigation.\textsuperscript{166} Identification of providers with outlying rates of utilization based on providers in the surrounding geographical area or with an outlying number of claims involving patients having traveled a larger-than-normal distance (serving as a proxy for “doctor shopping”) are two examples.\textsuperscript{167}

The best methods of fraud detection will be adaptive—systems that can learn and evolve their detection capabilities as new information and codes become available—while maintaining the ability to separate useful data from noise and to

\begin{itemize}
\item\textsuperscript{158} See Li et al., supra note 156, at 275.
\item\textsuperscript{159} See Wei Luo & Marcus Gallagher, \textit{Unsupervised DRG Upcoding Detection in Healthcare Databases}, ICDMW 2010: PROC. OF 10TH IEEE INT’L CONF. ON DATA MINING WORKSHOPS 600, 601 (2010).
\item\textsuperscript{160} See Tahir Ekin et al., \textit{Application of Bayesian Methods in Detection of Healthcare Fraud}.
\item\textsuperscript{161} See id. at 154.
\item\textsuperscript{162} See id. at 153.
\item\textsuperscript{163} See Li et al., supra note 156, at 281-82.
\item\textsuperscript{164} See Muhammad, supra note 156, at 63.
\item\textsuperscript{165} See Li et al., supra note 156, at 281–82; Luo & Gallagher, supra note 159, at 601; Marjorie A. Rosenberg et al., \textit{A Statistical Model to Detect DRG Upcoding}, 1 HEALTH SERV. & OUTCOMES RES. METHODOLOGY 233 (2000).
\item\textsuperscript{166} See Rasim M. Musal, \textit{Two Models to Investigate Medicare Fraud within Unsupervised Databases}, 37 EXPERT SYS. WITH APPLICATIONS 8628, 8629 (2010).
\item\textsuperscript{167} See id.
\end{itemize}
overcome deficiencies in the data. This will likely be achieved by systems that use a combination of supervised and unsupervised detection methods. However, both supervised and unsupervised data mining produce results that are essentially unusual patterns of potentially fraudulent activity. This implicates the prohibition against propensity evidence, while also raising questions about whether testimony concerning data mining, and the underlying statistical models, algorithms, and adaptive machine learning, is admissible expert testimony with sufficient foundational basis. Since the transition to the ICD-10 code set may change providers’ coding patterns due to increased coding errors or incidences of fraudulent coding activity, data-mined evidence may be at the forefront of the next wave of health care fraud litigation.

III. PROBLEMS OF STATISTICAL DETECTION EVIDENCE

Legal evidence may only reach the judge or jury if it meets the standards set forth in rules of evidence. The threshold requirement is almost always relevance. “Relevant” evidence is that which explanatory rather than merely argumentative. However, some evidence that may be relevant and sufficiently explanatory may nonetheless be “beyond the ken of the average juror”; in such instances, expert testimony is needed. Although all federal courts and several state courts currently follow Daubert, we lack consensus regarding the appropriate standard of admissibility for expert testimony. This is exemplified

168. See Li et al., supra note 156, at 284–85.
169. See id. at 276.
171. See FED. R. EVID. 402 (stating that all “relevant evidence is admissible unless . . . otherwise [provided] . . . . Irrelevant evidence is not admissible.”). “Relevant” evidence is that which has “any tendency to make a fact more or less probable than it would be without the evidence.” FED. R. EVID. 401.
173. See MCCORMICK ON EVIDENCE § 13, 29–31 (2d ed. 1972) (outlining that expert testimony is admissible only if the subject matter of the expert’s testimony is “so distinctively related to some science, profession, business or occupation as to be beyond the ken of the average layman,” and if the expert witness has “sufficient skill, knowledge, or experience in that field or calling as to make it appear this his opinion or inference will probably aid the trier in his search for truth”).
174. See Kristen Bolden, DNA Fabrication, A Wake Up Call: The Need to Reevaluate the Admissibility and Reliability of DNA Evidence, 27 GA. ST. U. L. Rev. 409, 428 (2011). Today, a majority of states employ Daubert entirely and explicitly, while many others do so implicitly or partially. See, e.g., Marron v. Stromstad, 123 P.3d 992, 1004 (Alaska 2005) (“But we have never adopted Kumho Tire’s extension of Daubert to all expert testimony . . . . [W]e limit our application of Daubert to expert testimony based on scientific theory, as opposed to testimony based upon the expert’s personal experience.”).
when the evidence involves statistical data or models such as the information
derived from and underlying data mining methods of fraud detection.\textsuperscript{176} Data
mining methods also implicate the reference class and blue bus problems
discussed in relation to statistical evidence being used to find liability.\textsuperscript{177}

\textbf{A. Scientific Reliability}

Problems concerning admissibility of expert evidence are illustrated by courts’
difficulties in and disagreement on the assessment of statistical evidence, even
though such evidence is supposed to simplify the modern adjudicative enterprise.\textsuperscript{178}
For example, testimony about the likelihood of DNA matches is common in criminal
trials, and statistical analysis is important in systemic employment discrimination
cases,\textsuperscript{179} but these and other similar cases commonly produce disputes.\textsuperscript{180}

\textsuperscript{176} See infra Part III.A.
\textsuperscript{177} See infra Part III. B.-C.
REV. 92, 93 (2009) (“The use of statistics is supposed to increase objectivity and rigor, yet . . .
statistics appear almost infinitely malleable . . . Indeed, rather than fulfill their promise as a neutral
basis for decisionmaking, statistics suddenly appear to be nothing but rhetorical tricks that
advocates can deploy in court.”). Historically, courts did not favor use of statistical, Bayesian, or
other forms of analysis, but this rigid disfavor has been criticized and often deemed inapplicable.
evidence code comprised of rigid, mechanistic rules, or for a lack of acceptance of statistical,
Bayesian, or other forms of analysis, derive from historical circumstances which no longer
apply.”).
the correct comparison group from which to determine if African Americans were sufficiently
underrepresented in the defendant’s workforce to suggest the standard operation of intentional
discrimination); \textit{Developments in the Law: Confronting the New Challenges of Scientific Evidence,
out that a common judicial misconception is that “judicial intuition can rectify a defective statistical
model by modifying the results of the hypothesis,” and using the example of \textit{EEOC v. O&G Spring
& Wire Forms Specialty Co.}, 38 F.3d 872, 888-89 (7th Cir. 1994), in which the dissent criticized
the majority’s finding of employment discrimination based solely on statistical evidence since the
underlying model may have failed to consider variables relevant to the definition of the defendant’s
labor market).
The general use of statistics is often governed by Daubert-like criteria. One of the earliest implications of this view was the appellate court’s ruling in People v. Collins, in which the prosecution’s expert witness attempted to use the product rule for allegedly independent characteristics. This was rejected on appeal as the expert’s statistical testimony lacked an adequate foundation both in evidence and in statistical theory, and the testimony and the manner in which the prosecution used it distracted the jury from its proper function of weighing the evidence on the issue of guilt. The first reason refers to the lack of justification offered for the almost arbitrarily chosen probability values as well as to the false assumption that the various characteristics were necessarily independent. The second reason is more elemental as it refers to the requirement that evidence be presented in such a way that it presents a fair measure of its strength. In other words, as later elucidated in Daubert, the statistical evidence must assist the trier of fact to understand or determine a fact in issue.

Data mining presents an extra challenge beyond the type of statistical evidence that was at issue in People v. Collins. This is because fraudulent activities such as upcoding involve a patient-specific, subjective determination of medical diagnosis or procedure by individual clinicians. Applying data mining detection methods to identify and label certain transactions as fraudulent or non-fraudulent—or, in essence, atypical of or conforming to what one would expect to see—threatens to make precise what is inherently imprecise, or to make

---

180. See, e.g., Cheng, supra note 178, at 93 (“In DNA cases, prosecutors often emphasize the random match probability (RMP), the probability that a person chosen at random from the population will have the same profile as the one found at the crime scene. Yet, what population is appropriate for calculating the RMP? The entire human population? The defendant’s racial subgroup? The city in which the crime occurred?”). See also State v. Spann, 617 A.2d 247, 257 (N.J. 1993) (“[U]se [of Bayes’ Theorem] in civil paternity proceedings appear to have legislative authorization . . . . [But] [o]pinions based on Bayes’ Theorem . . . are far from universally accepted for forensic purposes, especially in criminal cases.”).

181. See Weinstein’s Federal Evidence § 702.06, 4-702 (“The general standards for expert testimony also apply to statistical expert testimony; it is admissible only if the witness is qualified to give expert testimony in the field of statistics, the testimony will be helpful to the trier of fact, and the testimony is reliable and ‘fits’ the case.”). But see Daniel J. Capra, The Daubert Puzzle, 32 Ga. L. Rev. 699, 703 (1998) (stating that federal judges are not easily able to assess reliability of complex scientific testimony).


184. See id.

185. See id.


objective what is inherently subjective. However, this concern is mitigated by the fact that experts in litigation are still interpreting the results of data mining methods. The underlying models or algorithms are not making decisions or compelling testimony for the experts. Instead, data mining serves as a consultative or advisory tool to save time and provide consistency. This is particularly important given the scope of most health care fraud cases, which often deal with tens or hundreds of thousands of individual patient encounters, procedures, diagnoses, or records, which could not be practically reviewed one-by-one.

As an example to support this view, a federal district court recently allowed the U.S. government to extrapolate from a random sample for a considerably larger collection of claims in order to impose FCA liability against a health care corporation. The corporation owns over 200 skilled nursing facilities (SNFs) and was accused of violating the FCA by inappropriately pressuring its health care providers to target higher resource utilization group (RUG) levels and longer length-of-stay periods for patients (what could otherwise be characterized as selective upcoding) in order to maximize its Medicare reimbursement. In order to prove FCA liability, the government’s expert sought to use a random sample of 400 admissions from 82 SNFs spread over a seven-year period and then extrapolate the resulting statistical characteristics to a sample “universe” of over 50,000 patient admissions comprising over 150,000 individual claims.

The corporation argued that FCA liability could not be sufficiently demonstrated when expert testimony relies on statistical sampling and extrapolation. In particular, the corporation argued that it would be nonsensical to use such testimony to prove FCA liability because any one of the allegedly inappropriately coded patient encounters was the result of an “individual assessment of the patient’s clinical condition,” so extrapolation based on other patient encounters—not all of which were shown to be fraudulent themselves—was inapplicable.

190. See Katz, supra note 175, at 33.
191. See id.
192. See id.
196. See id. at *13.
197. See id. at *47 (“Defendant argues that, as the Government will only rely on statistical sampling and will not present evidence concerning patients’ actual conditions, diagnoses, clinical needs, the nature of therapy, or the extent of therapy, the Government cannot establish that the therapy provided to each patient was medically unnecessary.”).
However, the court rejected this argument on the grounds that use of statistical evidence met Daubert requirements, had become a conventional tool in litigation, and was particularly important in cases dealing with enormous amounts of data that could not practically be reviewed in their entirety. The use of a smaller portion of data to make statistical inferences about a larger, non-identical population was the exact point of statistical evidence. This is the same reasoning underlying unsupervised data mining methods, such as co-clustering models that allow detection of atypical or suspicious provider-beneficiary pairings. The court further disposed of the defendant’s due process arguments, clarifying that use of statistical evidence would not violate any rights to due process since the defendant retained tools to attack the weight accorded to any statistical evidence.

Thus, the two concerns indicated in People v. Collins—adequate foundation in statistics and assistance to the trier of fact to understand or determine a fact in issue—are addressed. Given that these issues were subsumed by the standard and admissibility guidelines outlined in Daubert, it is likely that testimony from experts with a sufficient background in statistics and data mining regarding

---

198. See id. at *18 (finding that the government’s statistical evidence was “based on reliable principles of statistics” and that the expert’s use of statistical models “indicate that the results will be within an acceptable degree of precision,” thereby meeting Daubert’s reliability requirement).

199. See United States v. Life Care Ctrs. of Am., Nos. 1:09-cv-251, 1:12-cv-64, 2014 WL 4816006, at *29–30 ("[S]tatistical sampling has become commonplace . . . In fact, courts now consider ‘mathematical and statistical methods [to be] well recognized as reliable and acceptable evidence in determining adjudicative facts.’")

200. See id. at *31, 45 ("[I]n view of the enormous logistical problems of [enforcement of government programs], statistical sampling is the only feasible method available . . . [and] the purpose of statistical sampling is precisely for these types of instances in which the number of claims makes it impracticable to identify and review each claim and statement.” (internal citations omitted)).

201. See id. at *49.

202. See Ekin et al., supra note 160, at 152.

203. See Life Care Ctrs. of Am., 2014 WL 4816006, at *59-60.

204. See Daubert v. Merrell Dow Pharm., 509 U.S. 579, 593–94 (1993). The Court provided a non-dispositive, non-exclusive, and flexible set of “general observation” that it considered relevant for established the “validity” of scientific testimony: (1) whether the theory or technique is falsifiable, refutable, and/or testable; (2) whether it has been subjected to peer review and publication; (3) the known or potential error rate; (4) the existence and maintenance of standards and control concerning its operations; and (5) the degree to which the theory and technique is generally accepted by a relevant scientific community. Id. Daubert was modified by General Electric Co. v. Joiner, 522 U.S. 136, 146 (1997) (holding that a district court judge may exclude expert testimony when there are gaps between the evidence relied upon by an expert and his or her conclusion, and that an abuse-of-discretion standard of review is the proper standard for appellate courts to use in reviewing a trial court’s decisions on admissibility of expert testimony) and Kumho Tire Co. v. Carmichael, 526 U.S. 137, 141 (1999) (holding that the trial judge’s gatekeeping function identified in Daubert applies to all expert testimony, including that which is non-scientific). For a more detailed discussion of whether evidence derived from data mining fraud detection methods is admissible under Daubert, the Federal Rules of Evidence, and the common law, see Caffrey, supra note 170.
results derived from data mining fraud detection methods meets scientific admissibility standards in health care fraud cases.

B. Reference Class Problem

Statistical evidence also concerns the so-called “reference class problem,” which forces one to consider the relationship between probability and weight of evidence; however, the use of data mining methods of fraud detection as a tool in an inductive reasoning process sufficiently addresses the problem to pass admissibility muster. The reference class problem stems from a simple observation: when we make statistical inferences about a specific individual or event, those inferences depend predominantly on how we group or classify that individual or event. But there is an infinite number of possible characteristics on which to base such grouping or classification, and ostensibly no principle to determine how to select or favor certain characteristics over others. As a result, statistics may become highly malleable. The resulting malleability has the potential to undercut the objectivity and certainty that make statistical evidence so promising and attractive for use in legal determinations.

This problem was famously illustrated by the case of United States v. Shonubi. In Shonubi, the defendant was caught entering the country at John F. Kennedy Airport with 427.4 grams of illegally smuggled heroin. He had made seven prior drug smuggling trips, but it was not known how much heroin he carried on those trips. The sentencing guidelines required the court to determine the total amount of heroin smuggled in the course of conduct (i.e., on the defendant’s eight trips combined). Accordingly, the court relied on a statistician’s estimate derived from customs service data on the amount of heroin recovered from 117 similar heroin smugglers apprehended at John F. Kennedy Airport during the time period in question.

The court’s reliance on such an estimate means the court believed the 117 individuals formed a “reference class” to which the defendant could reasonably be compared. However, why is this an appropriate reference class? The court could have simply multiplied the amount of heroin found on one trip by eight,

---

206. Id. at 92.
207. Id. at 2083.
208. Id.
209. Id. (citing Ronald J. Allen & Michael S. Pardo, The Problematic Value of Mathematical Models of Evidence, 36 J. LEGAL STUD. 107, 109 (2007)).
211. Id. at 464.
212. Id.
213. See id. at 466–67.
214. Id. at 468.
215. See id. at 510–11.
which places the defendant in a reference class on his own.\textsuperscript{216} The court also could have looked at how much heroin was carried by all passengers at John F. Kennedy Airport, which would likely yield a much lower number per person than apprehended heroin smugglers.\textsuperscript{217} In fact, the court could have selected any one of many hypothetical reference classes, each which would have produced a different result.\textsuperscript{218} The problem for courts is determining which reference class is the correct one on which to base liability.\textsuperscript{219}

Concerns regarding finding guilt based on a single statistic or probability have been discussed at length,\textsuperscript{220} and courts clearly do not find liability in this manner.\textsuperscript{221} While probabilities may contain relevant information to aid the trier of fact, they cannot establish liability alone if we have only one reference class without justification for its primacy over countless other plausible reference classes.\textsuperscript{222} Instead, courts use statistical probabilities to weigh the strength of different pieces of evidence, which may compel finding for one party or the other only when considered together.\textsuperscript{223} This, in part, is the basis for arguments

\begin{itemize}
\item \textsuperscript{216} See Cheng, supra note 205, at 2082. In fact, the original trial court, prior to appeal and remand, calculated the total amount of heroin smuggled on the eight trips in this manner—by multiplying the amount found on the last trip by the number of trips—to find the total to be 427.4 x 8 = 3,419.2 grams. United States v. Shonubi, 802 F. Supp. 859, 860–61 (E.D.N.Y. 1992).
\item \textsuperscript{217} See Cheng, supra note 205, at 2082.
\item \textsuperscript{218} The court may rely on a reference class to estimate a number, as in Shonubi, or to determine a probability of liability; both are problematic when only one reference class is considered. See Robert J. Rhee, Probability, Policy, and the Problem of the Reference Class, 11 INT’L J. EVID. & PROOF 286, 287 (2007) (“[T]he complication . . . is the problem of reference class. The rodeo attendees . . . could be categorized into ex-boy scouts and non-scouts, the former perhaps tending to be more honest. ‘That is, if the court were told all the circumstances relevant to the statistical probability of the man’s having bilked the rodeo organizers, the reference class for calculating this probability would be rather different.’” (citing L. JONATHAN COHEN, THE PROBABLE AND THE PROVABLE 78 (1977)); Mark Colyvan et al., Is it a Crime to Belong to a Reference Class?, 168 J. POLITICAL PHILOS. 168, 174 (2001) (“[S]ingle-case probabilities may not solve the [reference class problem].”)).
\item \textsuperscript{219} Some view the reference class problem as two distinct problems: a metaphysical problem and an epistemological problem. See Alan Hájek, The Reference Class Problem is your Problem too, 156 SYNTHESIS 563, 565 (2007) (“The former problem concerns what probabilities are ‘out there’ . . . . The latter problem concerns which probabilities should serve us as guides to life: which probabilities form appropriate bases for our inductive inferences and provide proper inputs to our decision-making. So perhaps we strictly should not speak of the reference class problem, as if there were only one problem.”).
\item \textsuperscript{220} See, e.g., Carl G. Wagner, Book Review of The Probable and the Provable by L. Jonathan Cohen, 1979 DUKE L.J. 1071, 1073 (1979) (“[Laurence Tribe] fears that if triers of fact were encouraged to think in explicit mathematical terms, they would give undue weight to statistical evidence (conveniently quantified for them by others) rather than attempt the difficult task of integrating such evidence with other relevant considerations to arrive at a fully informed subjective probability.”); Laurence H. Tribe, Trial by Mathematics: Precision and Ritual in the Legal Process, 84 HARV. L. REV. 1329, 1350, 1372 (1971) (referring to liability premised solely on probabilistic evidence as “inefficient,” “unfair,” and “intrinsically immoral.”).
\item \textsuperscript{222} See Rhee, supra note 218, at 289.
\item \textsuperscript{223} See id. at 288.
championing a process of inductive reasoning to find liability.\textsuperscript{224} Naked statistics alone carry little weight regarding overall liability, but they can help us understand and thereby measure the weight of individual pieces of evidence.\textsuperscript{225}

In the context of data mining methods of fraud detection, the main issue is identifying what is relevant among the enormous pool of health care information.\textsuperscript{226} But unlike lawyers arbitrarily selecting a reference class that will benefit their client’s case, many data mining methods can now easily implement automatic attribute selection that largely eliminates the reference class problem.\textsuperscript{227} Feature or attribute selection algorithms can eliminate redundant or unhelpful features from entire data sets before identifying potentially fraudulent data.\textsuperscript{228} These algorithms are similar in function to the model selection and feature selection methods advocated as solutions to the reference class problem.\textsuperscript{229} Moreover, studies have analyzed and compared various feature selection algorithms and methods to rank them based on accuracy and reduction.\textsuperscript{230} Furthermore, certain data mining methods of fraud detection have model selection built into their optimization procedures.\textsuperscript{231}

\textsuperscript{224} L. JONATHAN COHEN, THE PROBABLE AND THE PROVABLE 81 (1977). See also Stoljar, supra note 221, at 459 (“[T]he alternative to relying on the balance of probability to find liability is what Mr. Cohen calls ‘inductive probability,’ a form of reasoning . . . that offers a much better theoretical fit . . . For an inference to be inductively probable it must be derivable from a hypothesis or generalization that possesses adequate inductive support; more particularly, support based not on intuitive but on thoroughly empiricist grounds.”).


\textsuperscript{227} See, e.g., Josua Krause et al., INFUSE: Interactive Feature Selection for Predictive Modeling of High Dimensional Data, 20 IEEE Transactions on Visualization and Computer Graphics 1614, 1615 (2014) (explaining the importance of proper feature selection in predictive modeling); Ding-Wen Tan et al., The Impact of Feature Selection: A Data-Mining Application in Direct Marketing, 20 INTELL. SYS. ACC. FIN. MGMT. 23 (2013) (examining the impact of feature selection on neural networks and decision trees specifically); Hyunjung Shin et al., A Scoring Model to Detect Abusive Billing Patterns in Health Insurance Claims, 39 EXPERT SYS. WITH APPLICATIONS 7441, 7448 (2012) (proposing a scoring model that measures the abusiveness of healthcare providers in the medical services claims submitted to a payer that can integrate multiple attributes and identify the attribute most dissimilar from the norm); Patricia E.N. Lutu & Andries P. Engelbrecht, A Decision Rule-Based Method for Feature Selection in Predictive Data Mining, 37 EXPERT SYS. WITH APPLICATIONS 602, 602 (2010) (advocating a feature subset selection algorithm that selects features based on varying levels of correlation while eliminating noise).

\textsuperscript{228} See Lutu & Engelbrecht, supra note 227, at 609.

\textsuperscript{229} See Cheng, supra note 205, at 2095; Franklin, supra note 226, at 13.

\textsuperscript{230} See, e.g., Antonio Arauzo-Azofra et al., Empirical Study of Feature Selection Methods Based on Individual Feature Evaluation for Classification Problems, 38 EXPERT SYS. WITH APPLICATIONS 8170, 8175 (2011).

\textsuperscript{231} See, e.g., Siddhartha Bhattacharyya et al., Data Mining for Credit Card Fraud: A Comparative Study, 50 DECISION SUPPORT SYS. 602, 603 (2011).
Questions remain regarding whether algorithms consistently and correctly define relevance for each case. Nonetheless, it is clear that incorporation of feature and model selection into data mining algorithms largely placates reference class concerns since the algorithms are neither dictating nor compelling the expert’s testimony. Instead, the testifying expert must continue to meet scientific admissibility standards and the trier of fact merely weighs the strength of the evidence presented—rather than find liability outright—based on testimony regarding the algorithms underlying the determination of the best features or model selected to determine the reference class for the case in question.

C. Blue Bus Problem

Related concerns with the use of statistical evidence to find liability are illustrated by the classic “blue bus” example. In the hypothetical scenario, a driver is forced off the road at night by a bus. The driver was unable to identify the bus but nonetheless attempts to prove in civil litigation that the Blue Bus Company owned the bus and is thereby liable. The only evidence the driver presents is that the defendant bus company owns and operates 80% of all the buses in the city. The issue is whether this statistical probability alone is sufficient to find liability against the bus company for the accident in question. If a court finds the Blue Bus Company liable, then it should theoretically find the company liable in all similar accident cases even though the statistic presented suggests it would only be liable in, at most, 80% of cases.

However, liability cannot be found based on this form of naked statistical proof for efficiency and fairness reasons. Instead, there must be some

---

233. See supra Part III.A.
236. Nesson, supra note 235, at 1379.
237. Id.
238. Tribe, supra note 220, at 1341. Note that the reference class issue can also be illustrated with the Blue Bus example by changing the probability statistic to reflect the Blue Bus Company’s ownership of buses in the state, the country, or any geographical area beyond the city, or to change the reference class from ownership to the Blue Bus Company’s safety standards and protocols for reporting accidents. See Allen & Pardo, supra note 209, at 109–15.
239. See Tribe, supra note 220, at 1341.
240. See id. at 1350; Nesson, supra note 235, at 1379. It has been suggested that naked statistical evidence also raises Due Process concerns. See Alex Nunn, The Incompatibility of Due Process and Naked Statistical Evidence, VAND. L. REV. (forthcoming 2015). However, these concerns may be inapplicable to the Blue Bus problem, as assuming that Blue Bus Company continues to operate 80% of all buses on the road, it is possible—even minutely—that the company was indeed the liable party in every similar accident case brought to trial. See id. Alternatively, the Blue Bus Company could be compelled to pay 80% of the plaintiff-driver’s
additional evidence presented that connects the bus that caused the accident to the Blue Bus Company. 241 This is because the 80% statistic is merely a restatement of the probability or ratio of buses in the city owned by the company. It is not a statement about the probability of the specific accident that caused the plaintiff’s injuries. While a trier of fact may use the statistic to weigh the strength of the evidence, it is merely one factor in the preponderance test by which liability is found in civil cases. 242

A problem with this framework arises when we increase the naked probability statistic. What if the Blue Bus Company owned and operated 90% of the buses in the city? 243 99%? 99.99%? The question becomes at what point, if any, does the statement of probability alone permit an assertion about a specific accident. This question has arisen in cases of DNA prosecutions involving random match probabilities (RMPs) 244 or source probabilities, 245 in which it could be argued that probabilistic evidence can cross a threshold above which it is “transformed into [an] assertion of certainty rather than probability.” 246 In the
vast majority of such cases, courts have rejected challenges to the sufficiency of DNA evidence alone in determining liability or guilt.\textsuperscript{247}

In the context of data mining methods of fraud detection, the resulting data is produced by algorithms and models for which accuracy can be high enough—like DNA match statistics—for a trier of fact to treat the data as compelling proof.\textsuperscript{248} The view that a high probability of guilt or liability should compel admissibility of the evidence stems from a theory applied to DNA cases that has been dubbed the “exemplar cueing theory.”\textsuperscript{249} This theory posits that triers of fact tend to discount DNA match statistics when they can actually envision examples of other individuals in the population who might be innocent but still match the DNA profile (“coincidental match exemplars”).\textsuperscript{250} However, they will treat the DNA evidence as compelling proof of guilt or liability when they can no longer envision such alternative scenarios of innocence or non-liability.\textsuperscript{251}

In other words, as the possibility of error (or of implicating the aforementioned alternative scenario of non-liability) resulting from accepting the naked statistical evidence as sufficient proof approaches zero, the statistical evidence concerns illustrated by the blue bus problem similarly diminish.\textsuperscript{252} When supervised and unsupervised data mining methods are used to identify potentially fraudulent health care providers, there is no coincidental match exemplar. Instead, the only concerns are that providers committing coding fraud are not identified by the fraud detection methods (“false negative”) or that the providers labeled as fraudulent are, in fact, coding non-fraudulently (“false positive”).\textsuperscript{253} The former scenario is an issue of improving the data mining methods of detection and not an issue of evidentiary admissibility. The latter scenario is resolved by confining data mining fraud detection to the initial step of “flagging” providers as potentially fraudulent to make subsequent review of the data or investigation of the provider practical for human experts. Moreover, the same safeguards identified to trivialize the reference class problem apply here. Rather than the data-mined evidence compelling the expert’s testimony, the expert must continue to meet scientific admissibility standards,\textsuperscript{254} and the trier of fact merely uses the data to weigh the strength of the evidence presented. Thus, increases in detection accuracy rates of data mining methods of fraud detection evidence but of proof” given the power of DNA evidence to be “almost always decisive” in litigation).

\textsuperscript{247} See Roth, \emph{supra} note 244, at 1150; People v. Rush, 630 N.Y.S.2d 631, 634 (N.Y. Sup. Ct. 1995), \emph{aff’d}, 672 N.Y.S.2d 362 (App. Div. 1998) (finding that DNA evidence alone can establish a legally sufficient case of a defendant’s guilt).

\textsuperscript{248} See, e.g., Arauzo-Azofra et al., \emph{supra} note 230, at 8175.

\textsuperscript{249} See Jonathan J. Koehler, \emph{When Are People Persuaded by DNA Match Statistics?} 25 \textsc{Law \\& Human Behavior} 493, 495 (2001).

\textsuperscript{250} Id.

\textsuperscript{251} Id.

\textsuperscript{252} See Roth, \emph{supra} note 244, at 1169.

\textsuperscript{253} See Aral et al., \emph{supra} note 253, at 39.

\textsuperscript{254} See \emph{supra} Part III.A.
achieved by, for example, improved feature and model selection simultaneously address blue bus concerns related to admissibility of statistical evidence.

D. Propensity

Data mining methods of fraud detection produce results that are essentially unusual patterns of potentially fraudulent activity, which raises concerns that the results would be inadmissible as propensity evidence, though the results may be justified under the doctrine of chances. Federal Rule of Evidence 404(b) outlines a character propensity rule, under which evidence is inadmissible “to prove a person’s character in order to show that on a particular occasion the person acted in accordance with the character.”255 However, when an act is committed repeatedly in a particular way (such as recurrent coding practices that may be classified as upcoding), courts typically will permit evidence of each act regardless of whether the acts were all planned together.256 In other words, such evidence does not fall under the purview of the ban on character propensity. In addition, there is no requirement for a “master plan” as long as the blueprint or modus operandi of each unrelated act appears to be sufficiently similar.257

Thus, in a classic case informally dubbed the “Brides of the Bath” case, the fact that several previous wives of the defendant were found drowned in a bathtub was admitted as evidence in his murder trial for the death of one particular wife who similarly drowned in a bathtub.258 Some might view this as showing the defendant’s “specific propensity,” which is distinct from the aforementioned character propensity banned by Federal Rule of Evidence 404(b).259 The trait of drowning one’s wives in the bathtub is not meant to impermissibly raise the specter of general negative propensity or character (i.e., that the defendant is an immoral and homicidal person and likely acted in accordance with that trait in committing the crime in question), but rather to show that he has a specific propensity to intentionally drown his wives in the bathtub, and likely acted in accord with that specific propensity.260 Thus, the court did not view the defendant as having a “character” to drown his wives in the bathtub, since character refers to a very general propensity (immorality,

---

255. Fed. R. Evid. 404(b)(1). Admissible purposes for evidence include, but are not limited to, proving motive, opportunity, intent, preparation, plan, knowledge, identity, absence of mistake, or lack of accident. Fed. R. Evid. 404(b)(2).
260. See id.
violence, lawlessness, etc.).\footnote{261} However, the court did believe he may have a specific propensity to do so.\footnote{262}

Professor Paul Rothstein has argued that character is not synonymous with propensity, but simply one type of propensity: one that is "amorphous, diffuse, and tinged with moral approbation or disapprobation."\footnote{263} Accordingly, he distinguishes the specific propensity to repeatedly do a certain thing in a certain way, from the general character that is prohibited by the Federal Rules of Evidence.\footnote{264} A related but different view is held by Professor Edward Imwinkelried, who eschews Professor Rothstein's partition of propensity into types and instead argues that admitting evidence of prior similar conduct of a defendant without invoking the ban on character evidence (or even invoking propensity) is justified by the "doctrine of chances."\footnote{265} Under this doctrine, the trier of fact evaluates the odds of an innocent person being repeatedly involved in similar suspicious circumstances by coincidence or chance, rather than focusing on the individual as a potentially immoral or bad person.\footnote{266}

The paradigmatic case applying the doctrine of chances is \textit{United States v. Woods}, in which the defendant was charged with the death of a child in her care.\footnote{267} Evidence existed that a number of children previously in her care had also died mysteriously.\footnote{268} The likelihood that the current death was accidental decreased with the existence of so many other unrelated but similar deaths.\footnote{269} Thus, the jury could infer that the probability of so many accidental deaths happening to the same person was extremely small, without inferring that the defendant had a bad character or even a propensity to commit the crime.\footnote{270}
Professor Rothstein has responded to this characterization by explaining that the doctrine of chances is in fact premised on a propensity-based framework under which innocent people act differently than guilty people.\textsuperscript{271} It is only because of a once-guilty person’s propensity to repeat that the probability of present guilt is higher for that person.\textsuperscript{272} Otherwise, it would be equal to the probability of present guilt of a previously uninvolved person.\textsuperscript{273}

In the context of data mining, results that “flag” claims or providers for secondary, individualized investigation can be characterized under and deemed admissible by the doctrine of chances as described by Professor Imwinkelried and other proponents of the theory.\textsuperscript{274} Evidence of multiple similar but independently improbable events supports an objective, statistical inference of lack of accident or random chance on a particular occasion—that is, an inference of purposive action or intent.\textsuperscript{275} Upcoding, collusion between providers or between providers and patients, and medical treatment items uncharacteristically shifting from one cluster to another over short periods of time all entail patterns of individual acts that, when considered together, become less probable to occur by coincidence or chance the more acts there are in the pattern.\textsuperscript{276} This traces the reasoning of the doctrine of chances.

Fear that such evidence would be unduly prejudicial is mitigated by confining data mining fraud detection to the initial step of “flagging” providers as potentially fraudulent to make subsequent review of the data or investigation of the provider practical for human experts. While a defendant’s claim of accident becomes less believable if the defendant has incurred the same error more frequently than the typical, innocent person,\textsuperscript{277} a second step of human review theoretically should differentiate the truly fraudulent cases (“true positives”) from the cases where fraud was erroneously identified by data mining (“false positives”). Finally, Professor Rothstein’s partition of propensity into types is less applicable in the data mining context. It would be more difficult for government prosecutors to prove that health care providers identified as potentially fraudulent by data mining methods of fraud detection have the “specific propensity” to fraudulently code or diagnose.

\textsuperscript{271} See Rothstein, supra note 259, at 1262–63.
\textsuperscript{272} Id. at 1263.
\textsuperscript{273} Id.
\textsuperscript{274} See id.
\textsuperscript{275} See Sullivan, supra note 265.
\textsuperscript{276} See United States v. Woods, 484 F.2d 127, 135 (4th Cir. 1973) (“[T]he incidents must be considered collectively, and when they are, an unmistakable pattern emerges. That pattern overwhelmingly establishes defendant’s guilt.”).
\textsuperscript{277} See Imwinkelried, supra note 257, at 78 (citing Edward J. Imwinkelried, The Use of Evidence of an Accused’s Uncharged Misconduct to Prove Mens Rea: The Doctrine Which Threatens to Engulf the Character Evidence Prohibition, 51 OHIO ST. L.J. 575, 590–93 (1990)).
IV. Conclusion

The transition to ICD-10 has raised many concerns over the past decade, with some fearing that it will facilitate or increase the potentially devastating liability that health care providers face under the False Claims Act. Given the exponential increase in the number and detail of codes, as well as the problems inherent with medical coding such as insufficient coding training and a lack of unanimity in coding among both health care providers and professional coders, there is likely to be an increase in incidences of inadvertent coding error or fraudulent coding activity such as upcoding. Supervised and unsupervised data mining methods can be applied to the field of fraud detection by analyzing massive collections of health care records and identifying unusual patterns of potentially fraudulent activity. Despite concerns of such statistical fraud detection relating to scientific admissibility, reference class selection, the blue bus problem, and propensity, the use of statistical evidence derived from data mining is likely admissible in court since the debate over the use of statistical evidence is “not one of exclusion, but rather one of appropriate weight.”

An expert testifying about data mined results is essentially testifying about what an algorithm or statistical model has inferred about a defendant’s likely state of mind. In addition, the expert would interpret the results and testify about both his background to satisfy expert witness requirements and the models and algorithms underlying the data mining process to satisfy scientific admissibility standards of, inter alia, relevance and reliability. Moreover, probabilistic evidence can theoretically cross a threshold above which can be reasonably relied upon as an assertion of certainty sufficient for admissibility. Thus, rather than expecting triers of fact to determine liability based on the statistical data itself, data mining serves as an important tool that allows analysis of data that would otherwise be impossibly laborious and that allows more accurate measurement of the weight of evidence. Given the sheer scale of health care fraud—a scale that will undoubtedly grow with the transition to ICD-10—data mining methods of fraud detection are becoming systematically more advanced and look to feature more prominently in litigation than ever before.

278. Rhee, supra note 218, at 291 (citing Allen & Pardo, supra note 209).
279. See generally Caffrey, supra note 170.
THE FICTION OF PRIVACY UNDER THE FOURTH AMENDMENT: 
EXAMINING WARRANTLESS CELL PHONE SEARCHES IN THE 
CONTEXT OF RILEY V. CALIFORNIA

Casey A. Taylor*

I. INTRODUCTION

In the face of novel and ever-changing technology, the law continues to meet 
new challenges almost daily. With every updated version of computer software 
and new generation of the iPhone, comes a new hurdle or situation begging for 
legal analysis.1 In 2013, ninety-one percent of adults in the United States 
reported that they owned a cell phone.2 Fifty-eight percent reported that they 
owned a smart phone.3 Of the total number of cell phone owners, eighty-one 
percent sent and received text messages, sixty percent accessed the internet, fifty-
two percent sent and received emails, and fifty percent downloaded apps.4 These 
numbers are constantly increasing, evidencing the growth and prevalence of 
technology in our everyday lives.5 Additionally, many cell phones allow their 
users to take photos, keep track of their appointments on a calendar, and much 
more. Thus, the cell phone serves as an electronic footprint that documents 
online activity, places traveled, and people spoken to, as well as the information 
itself posts to social media sites.

According to a recent survey, “accessing social media is the number one 
mobile activity today.”6 Of the social media sites examined, Facebook ranked as 
the most dominant, with seventy-five percent of people using mobile technology 
to access it, followed by Twitter at twenty-eight percent, and Instagram at 
thirteen percent.7 Facebook, like other social media sites, allows its users to

* J.D. candidate 2016 at the Salmon P. Chase College of Law at Northern Kentucky 
University.
1. See Marc Rotenberg & Alan Butler, In Riley v. California, a Unanimous Supreme Court 
Sets Out Fourth Amendment for Digital Age, SCOTUS BLOG (June 26, 2014, 6:07 PM), 
http://www.scotusblog.com/2014/06/symposium-in-riley-v-california-a-unanimous-supreme-court-
sets-out-fourth-amendment-for-digital-age/.
2. Maeve Duggan, Cell Phone Activities 2013, Internet, Sci. & Tech., P
3. Mobile Technology Fact Sheet, Internet, Sci. & Tech., P
4. Duggan, supra note 2.
5. See id. (The percentage of cell phone owners/users who download apps on their phones is 
up thirty-eight percent from that which was reported in 2009).
6. Ray Pun, Adobe 2013 Mobile Consumer Survey: 71% of People Use Mobile to Access 
7. Id.
share some of their most personal and intimate information, such as their interests, work history, and photos.\(^8\)

Part II of this paper examines prior legislation and case law governing the issue of warrantless searches and how they apply to modern technology. Prior courts have generally allowed warrantless searches pursuant to exceptions to the Fourth Amendment, but placed limitations on those exceptions.\(^9\) On June 25, 2014, in *Riley v. California*, the United States Supreme Court issued a ruling requiring that law enforcement obtain a warrant prior to any cell phone search incident to an arrest.\(^10\) *Riley* addressed the contradictory rulings of the California Court of Appeals and the First Circuit regarding the admissibility of evidence extracted during cell phone searches.\(^11\) In its decision, the Supreme Court reasoned that modern cell phones contain a plethora of information about one’s life and that, given the extensive amount of information left vulnerable to a search, privacy was of the utmost concern.\(^12\)

The Court examined Fourth Amendment rights against unreasonable searches and seizures and analyzed the Fourth Amendment’s recognized exceptions, such as when an officer’s safety is jeopardized or when evidence is at risk of being lost or destroyed.\(^13\) However, the Court ultimately concluded that “data on [a] phone can endanger no one” and that the risk of evidence being lost or destroyed could be mitigated by means other than a search, such as by powering off the cell phones or by placing the cell phones in bags that restrict electronic waves necessary for a remote wiping of the phone’s data.\(^14\) The Court’s decision has sparked discussion as to the impact that will inevitably follow for other forms of technology.\(^15\)

Part III provides an overview and analysis of the recent Supreme Court decision in *Riley v. California*. While the Constitution provides protections against law enforcement warrantless cell phones searches,\(^16\) prior to the Court’s decision in *Riley*, law enforcement easily circumvented this protection through

---

9. See, e.g., United States v. Ziller, 623 F.2d 562, 563 (9th Cir. 1980) (permitting the search of a wallet found on the arrestee’s person); United States v. Rosenthal, 793 F.2d 1214, 1232 (11th Cir. 1986) (permitting the search of a bag that the arrestee was moving toward at the time of arrest); United States v. Weaver, 433 F.3d 1104, 1105 (9th Cir. 2006) (permitting the search of a personal organizer located behind the driver’s seat of a vehicle).
11. See id. at 2480-82.
12. See id. at 2495. (“[T]he fact that technology now allows an individual to carry such information in his hand does not make the information any less worthy of the protection for which the Founders fought.”).
13. Id. at 2496.
14. Id. at 2480, 2487
16. See U.S. CONST. amend. IV.
recognized exceptions to the Fourth Amendment. The Supreme Court overruled these exceptions and required that law enforcement obtain a warrant prior to conducting any cell phone search, even those incident to arrest, thereby preserving the idea that cell phone users are entitled to a certain degree of privacy. But what protections are in place for obtaining the same information contained on a cell phone (such as text messages, emails, photos, social media posts, etc.) through other avenues? Much of this same information is available elsewhere without a warrant and is thus unprotected by the probable cause standard. Part IV examines these other avenues of obtaining information. Part V argues that the accessibility of information through such other avenues renders Riley somewhat meaningless. Despite the decision and idealistic reasoning of the Court in Riley, requiring a warrant in order to search a cell phone is seemingly futile considering the accessibility of the same data elsewhere.

Part VI explores how Riley applies to various forms of technology, which are becoming increasingly prevalent in today’s society, as well as other methods by which law enforcement may obtain digital information. This portion of the paper asserts the necessity of addressing such issues proactively so as to avoid the same inconsistency and confusion that was present prior to the Riley decision. Part VI also notes the implications of the law’s current state and suggests ways in which the law should treat future searches of technology, not limited to the devices themselves, but also the information they contain. This note concludes by asserting that administrative subpoenas should be abolished in the interest of maintaining the Fourth Amendment’s right to privacy.

17. See United States v. Lustig, 3 F. Supp. 3d 808, 817 (S.D. Cal. 2014) (quoting United States v. Wurie, 728 F.3d 1, 3-4 (1st Cir. 2013)) ("[T]he search-incident-to-arrest exception permits an arresting officer ‘to search for and seize any evidence on the arrestee’s person in order to prevent its concealment or destruction’ and to search ‘the area into which an arrestee might reach in order to grab a weapon or evidentiary items.’"). See also United States v. Schesso, 730 F.3d 1040, 1050-51 (9th Cir. 2013) (quoting Herring v. United States, 555 U.S. 135, 143 (2009)) ("[E]vidence should be suppressed ‘only if it can be said that the law enforcement officer had knowledge, or may properly be charged with knowledge, that the search was unconstitutional under the Fourth Amendment.’").

18. Lustig, 3 F. Supp. 3d at 817 (citing United States v. Quintana, 594 F. Supp. 2d 1291, 1299 (M.D. Fla. 2008)) ("[A] cell phone owner generally has a reasonable expectation of privacy in the content of electronic information stored in his phone."); Riley v. California, 134 S. Ct. 2473, 2493 (2014) ("[A] warrant is generally required before such a search, even when a cell phone is seized incident to arrest.").

II. PRIOR LEGISLATION AND CASE LAW GOVERNING WARRANTLESS SEARCHES

A. The Fourth Amendment

The Bill of Rights was written in order to “place specific limits on government power” and in response to several states’ outcries for greater “protection of individual liberties.”\(^{20}\) The Fourth Amendment reads in relevant part: “[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause[.]”\(^{21}\) It is well-settled law that the Fourth Amendment protects individuals against “arbitrary invasions by government officials.”\(^{22}\) A plain reading of the Fourth Amendment in the present context, however, is more complex than it seems. First, one must determine if the alleged action taken by law enforcement constitutes a search.

A search occurs when a government entity violates “an expectation of privacy that society is prepared to consider reasonable.”\(^ {23}\) This definition has been broken down into two separate inquiries: first, whether the individual who is the subject of the investigation has “manifested a subjective expectation of privacy[]”; and second, whether society characterizes that expectation of privacy as reasonable.\(^ {24}\)

The Fourth Amendment focuses on the component of reasonableness, as it protects only against “unreasonable searches and seizures.”\(^ {25}\) Once it is determined that a search occurred of an area one expects to be private, and that his or her expectation was reasonable by societal standards, the government bears the burden of showing that a warrantless search was permissible under the circumstances.\(^ {26}\) A cell phone user generally has a reasonable expectation that the content of their cell phone will remain private.\(^ {27}\) Moreover, “[a] warrantless search is per se unreasonable unless one of the few exceptions applies.”\(^ {28}\) An unreasonable search does not automatically preclude the information obtained by


\(^{21}\) U.S. CONST. amend. IV.


\(^{24}\) Warshak, 631 F.3d at 284 (quoting California v. Ciraolo, 476 U.S. 207, 211 (1986)) (citing Smith v. Maryland, 442 U.S. 735, 740 (1979)).

\(^{25}\) See U.S. CONST. amend. IV.


\(^{28}\) Id. at 816.
that search from being used as evidence or render it inadmissible in court. This idea is known as the exclusionary rule, which requires the exclusion of evidence only “when the police exhibit deliberate, reckless, or grossly negligent disregard for Fourth Amendment rights.”

The exclusion of evidence is not a first impulse; therefore, the exclusionary rule is somewhat of a “last resort.” Instead, there are a few specific exceptions, which, if present, disallow the suppression of such evidence, including the notable and relevant “good faith,” “search-incident-to-arrest,” and “exigent circumstances” exceptions.

1. The “Good Faith” Exception

The good faith exception became prominent after the Supreme Court’s decision in Davis v. United States. In Davis, officers conducting a routine traffic stop learned that the driver of the vehicle had lied to them about his name. The officers arrested the driver, secured the scene, and subsequently searched the car, relying on then-existing precedent permitting the search of a vehicle incident to arrest. The officers found a revolver in the car, and the driver was found guilty of being a felon in possession of a firearm.

The Supreme Court, in a case decided after Davis’s arrest but before his appeal, set forth new rules governing vehicle searches incident to the occupant’s recent arrest, and Davis raised the issue on appeal. However, the Supreme Court found that “searches conducted in objectively reasonable reliance on binding appellate precedent are not subject to the exclusionary rule.” The Davis ruling was ultimately affirmed because the officers in that case had relied upon precedent in effect at the time of the search. The good faith exception is

---

29. Id. at 819 (quoting Herring v. United States, 555 U.S. 135, 143 (2009)) (“The fact that a Fourth Amendment violation occurred - i.e., that a search or arrest was unreasonable - does not necessarily mean that the exclusionary rule applies”).
30. United States v. Aguiar, 737 F.3d 251, 259 (2d Cir. 2013) (quoting United States v. Stokes, 733 F.3d 438, 443 (2d Cir. 2013)).
31. Id. (citing Herring, 555 U.S. at 140).
32. See United States v. Wurie, 728 F.3d 1, 3 (1st Cir. 2013) (discussing the “search-incident-to-arrest” exception). See also Lustig, 3 F. Supp. 3d at 819 (discussing the “good faith” exception); Ashley B. Snyder, Comment., The Fourth Amendment and Warrantless Cell Phone Searches: When is Your Cell Phone Protected?, 46 WAKE FOREST L. REV. 155, 173-74 (2011).
33. See generally Davis v. United States, 131 S. Ct. 2419 (2011) (allowing a warrantless search when law enforcement relied in good faith on precedent in existence at the time of the search).
34. Id. at 2421-22.
35. Id. at 2422.
36. Id.
37. Id. See generally Arizona v. Gant, 556 U.S. 332 (2009) (holding that a search incident to arrest was not proper if the arrestee could not reach into the area being searched).
still recognized, but the government bears a “heavy burden” of showing that it applies.\footnote{40} 

2. The “Search-Incident-to-Arrest” Exception

Another exception to the Fourth Amendment exclusionary rule is the search-incident-to-arrest exception.\footnote{41} This exception provides that law enforcement may search any item within the “immediate control” of the arrestee.\footnote{42} The premise behind this exception is that, once a person is lawfully arrested, he or she has a lower expectation of privacy.\footnote{43} A 2009 Supreme Court decision extended this exception to vehicles when the arrestee is within close enough proximity to the vehicle that he or she “might gain possession of a weapon or destructible evidence.”\footnote{44}

Since the search-incident-to-arrest exception’s creation, however, there has been little monitoring for its abuse.\footnote{45} In many instances, law enforcement officers have not needed to show that they had reason to believe any such threat or evidence ever existed.\footnote{46} Additionally, the exception extends to highly personal items, such as wallets, bags, and personal organizers,\footnote{47} and was also interpreted by the Supreme Court in \textit{Gant} to include cell phones.\footnote{48} The only clear and consistent limitations to this exception are its spatial and temporal limits – specifically, a warrantless search is permitted only “contemporaneous with the arrest and . . . [in] the immediate vicinity of the arrest.”\footnote{49} Therefore, if a warrantless search is conducted of an area not in the vicinity of the arrest or

\begin{itemize}
\item \footnote{40. United States v. Wurie, 728 F.3d 1, 13 (1st Cir. 2013) (quoting United States v. Syphers, 426 F.3d 461, 468 (1st Cir. 2005)).}
\item \footnote{41. United States v. Gomez, 807 F. Supp. 2d 1134, 1142 (S.D. Fla. 2011)).}
\item \footnote{42. Id. (citing Chimel v. California, 395 U.S. 752, 763 (1969)).}
\item \footnote{43. Id. (citing United States v. Robinson, 414 U.S. 218, 233-24 (1973)).}
\item \footnote{44. See Chimel, 395 U.S. at 763. See also generally Arizona v. Gant, 556 U.S. 332 (2009) (upholding search of vehicle only if arrestee was in close enough proximity to the vehicle to reach into it).}
\item \footnote{45. See Gomez, 807 F. Supp. 2d at 1143 (citing United States v. Jackson, 377 F.3d 715, 716 (7th Cir. 2004)) (“[O]bjects found on an arrestee’s person, on his clothing, on any area within his immediate control, may be searched by law enforcement, with or without any reason to suspect that the person is armed or carrying contraband.”).}
\item \footnote{46. Id.}
\item \footnote{47. See, e.g., United States v. Ziller, 623 F.2d 562, 563 (9th Cir. 1980) (permitting the search of a wallet found on the arrestee’s person); United States v. Rosenthal, 793 F.2d 1214, 1232 (11th Cir. 1986) (permitting the search of a bag that the arrestee was moving toward at the time of arrest); United States v. Weaver, 433 F.3d 1104, 1105 (9th Cir. 2006) (permitting the search of a personal organizer located behind the driver’s seat of a vehicle).}
\item \footnote{48. Gant, 556 U.S. at 332.}
\item \footnote{49. United States v. Gomez, 807 F. Supp. 2d 1134, 1144 (S.D. Fla. 2011) (quoting Holmes v. Kucynda, 321 F.3d 1069, 1082 (11th Cir. 2003)).}
\end{itemize}
substantially after the arrest occurs, it is does not fall under the search-incident-to-arrest exception and is considered unreasonable and invalid.50

3. The “Exigent Circumstances” Exception

The exigent circumstances exception is yet another notable exception to the Fourth Amendment exclusionary rule, under which evidence acquired during a warrantless search might be admissible in court.51 This exception permits law enforcement to conduct a search without a warrant any time there is a reasonable belief that the delay necessary to obtain a warrant would result in the destruction of potential evidence.52 Courts have considered this exception in the context of cell phones by analyzing whether a search of a cell phone’s call history, text messages, and images was justified due to the threat of such contents being deleted from the phone.53 The law enforcement community has historically argued that a search is necessary to prevent the destruction of evidence because, as new calls and messages come into the phone, older ones may be automatically deleted.54 This reasoning was initially inspired by the idea that pagers deleted older data in a similar fashion; however, the courts that accepted this logic did not account for the technical differences between cell phones and pagers.55 Some courts have since determined that while pagers delete information in a “first-in, first-out” fashion, cell phones are vastly different and ruled that, due to these differences, there is essentially no risk of evidence being destroyed in the time it takes to procure a warrant.56 The basis for the exigent circumstances exception is essentially encompassed by the search-incident-to-arrest exception.57 The critical difference between the two exceptions is that “unlike the search incident to arrest exception, the exigent circumstances exception requires a court to examine whether an emergency justified a warrantless search in each particular case.”58

50. See id. (citing United States v. Wells, 347 F.3d 280, 287 (8th Cir. 2003)) (holding the search of a vehicle invalid when the vehicle was driven to the station after the arrest, but prior to the search).
51. Id. at 1150 (citing United States v. Santana, 427 U.S. 38, 43 (1976)).
52. Snyder, supra note 32, at 173-74 (citing State v. Carroll, 778 N.W.2d 1, 9 (Wis. 2010)).
53. Id. at 174.
54. Id. (citing United States v. Santillan, 571 F. Supp. 2d 1093, 1101 (D. Ariz. 2008)).
55. Id. See also United States v. Wall, No. 08-60016-CR, 2008 WL 5381412, at *3 (S.D. Fla. Dec. 22, 2008) (discussing how previous courts did not explain why cell phones and pagers should be treated similarly).
56. See generally Wall, 2008 WL 5381412, at *1 (discussing the differences between pagers and cell phones and noting that the exigent circumstances no longer applies to such technology).
57. See Park, supra note 26, at 440 (“The two general exigencies justifying the warrantless search incident to arrest of the person are (1) to ensure officer safety and (2) to prevent the concealment or destruction of evidence.”).
B. The History of Warrantless Searches

The Supreme Court first provided concrete rules for limiting warrantless searches under the Fourth Amendment in its *Chimel* decision. The Court justified such searches when either it was necessary for the officer to search the area and remove objects that the arrestee might use to resist arrest, escape, or physically harm the officer, or when evidence was at risk of concealment or destruction. The *Chimel* decision also provided spatial limitations surrounding the rule, declaring that the aforementioned searches of the arrestee’s person and areas within the arrestee’s immediate control were permissible. The Court interpreted “immediate control” as “the area from within which he might gain possession of a weapon or destructible evidence.” This area is commonly referred to as the “grab zone.” The search in *Chimel* was ultimately found to be unreasonable because of these spatial limitations. The Court ruled that it was improper for officers to search the entire home of a man arrested for burglary without a warrant, including rooms other than that in which he was arrested, because they were not in the immediate control, or “grab zone,” of the arrestee. Therefore, there was no threat of harm or destruction of evidence.

Four years after *Chimel*, the Court addressed what proof or support is required for officers to show there was a risk of harm or destruction of evidence that justified their warrantless search. The Court essentially dismissed the question, finding that a search incident to arrest is usually a “quick ad hoc” judgment, and that the search should not be subject to “what a court may later decide was the probability in a particular arrest situation that weapons or evidence would in fact be found upon the person of the suspect,” but rather, requires no justification. A few years later, the Court altered its stance on this matter, holding that a search absent any exigencies was unreasonable.

The Supreme Court noted in *New York v. Belton* that the search of a container incident to arrest, even when located within a vehicle, is permissible. The Court explained that such a search was valid whether the container was open or closed because the arrest “justifies the infringement of any privacy interest the

---

59. See generally *Chimel v. California*, 395 U.S. 752 (1969) (discussing the scenarios in which it would be reasonable for an officer to conduct a search absent a warrant).
60. *Id.* at 763.
61. *Id.*
62. *Id.*
63. Park, *supra* note 26, at 437.
64. *Chimel*, 395 U.S. at 768.
66. *Id.*
69. Park, *supra* note 26, at 436 (citing United States v. Chadwick, 433 U.S. 1, 11 (1977)).
arrestee may have.”  

In a much more recent decision, however, the Court noted that, while the Belton court did not address whether or not the searches of vehicle’s passenger compartments are valid irrespective of whether the area searched is within the “grab zone” during the time of the search or during the time of the arrest, its decision would limit passenger compartment searches to those areas within the “grab zone” at the time of the search. This decision ties in to the exigency requirement of Chadwick because once the subject of the search is arrested and secured, there is no longer a threat of him or her harming the officers or destroying evidence within the “grab zone.” The Court further noted that it had legitimate concerns regarding law enforcement’s unbridled rummaging through citizens’ vehicles. Justice Scalia even went so far as to express his belief that vehicles should not be searched at all unless there is reason to believe that the vehicle contains evidence related to the crime for which the arrestee was arrested. However, it is somewhat uncertain whether this rule applies to all searches-incident-to-arrest or only to vehicular searches.

The Supreme Court decisions discussed above constituted the law in regards to warrantless searches-incident-to-arrest prior to Riley v. California. Officers could search the person of an arrestee or the area within his or her immediate control or “grab zone,” including both open and closed containers found in those areas. Searches of vehicles were also permitted without a warrant if the arrestee was unsecured and the officer had reason to believe the vehicle contained evidence related to the arrest. There were essentially two exigencies, one of which had to be present to justify a warrantless search. The first was a risk to officer safety. The second was the potential for evidence to be destroyed or concealed.

C. Cell Phones and Warrantless Searches Under the Search-Incident-to-Arrest Exception

Previous courts, most notably the Fifth Circuit in United States v. Finley, have deemed warrantless searches of cell phones as reasonable under the search-incident-to-arrest exception, reasoning that a cell phone is indistinguishable from

---

71. Id. at 461.
73. See id.
74. See id. at 344-45.
75. Park, supra note 26, at 439 (citing Thornton v. United States, 541 U.S. 615, 632 (2004) (Scalia, J., concurring)).
76. Id. at 440 (citing United States v. Curtis, 635 F.3d 704, 713, 713 n.22 (5th Cir. 2011), cert. denied, 132 S. Ct. 191 (2011)).
77. Id.
78. Id.
79. Id.
80. Id.
81. Park, supra note 26, at 440.
any other container.\textsuperscript{82} While the defendant in \textit{Finley} contended that, because the cell phone was “closed,” law enforcement did not have the authority to search its contents, the Fifth Circuit held that the cell phone was a container found on the arrestee’s person at the time of the arrest and that precedent allowed for the search of containers, whether open or closed, found on the person of the arrestee during a lawful arrest.\textsuperscript{83} Some jurisdictions have upheld this logic, further reasoning that the digital information on cell phones is not qualitatively different than the same information in hard-copy form; thus, the physical cell phone merely acts as a container for that digital information.\textsuperscript{84}

However, many jurisdictions have refused to extend the container analysis to cell phones, focusing on the large amount and personal nature of information that cell phones are capable of holding, the inability of officers to access the information stored in a cell phone from its exterior, and a cell phone’s inability to hold tangible items.\textsuperscript{85} Irrespective of the container analysis, courts have also rejected warrantless cell phone searches on the grounds that once the cell phone is in police custody, it can no longer be used to harm anyone and the arrestee can no longer destroy evidence that might be stored on it.\textsuperscript{86} Other jurisdictions have found the determination of whether a cell phone is a container irrelevant because past courts have held the search of non-container items was valid so long as they met the other requirements of the search-incident-to-arrest exception, thus allowing searches of cell phones incident to a lawful arrest.\textsuperscript{87}

\textbf{III. \textit{Riley v. California}}

The contradicting opinions among the courts and the rapid growth of technology have made the need for consistency obvious. That is what the \textit{Riley v. California} decision provided. In \textit{Riley}, the petitioner was stopped for a traffic violation and later arrested on weapons charges.\textsuperscript{88} During his arrest, the arresting officer found and seized a cell phone from Riley’s pocket.\textsuperscript{89} The officer began searching the cell phone and recognized a term associated with a local street gang

\begin{itemize}
\item \textsuperscript{82} Id. at 442 (citing United States v. Finley, 477 F.3d 250, 260, 260 n.7 (5th Cir. 2007)).
\item \textsuperscript{83} Id. (citing \textit{Finley}, 477 F.3d at 260 (citing United States v. Robinson, 414 U.S. 218, 235 (1973))).
\item \textsuperscript{84} See, \textit{e.g.}, Fawdry v. State, 70 So. 3d 626, 630 (Fla. Dist. Ct. App. 2011).
\item \textsuperscript{85} See, \textit{e.g.}, Park, supra note 26, at 444-45 (citing United States v. Park, No. CR 05-375 SI, 2007 WL 1521573, at *8 N.D. Cal. May 23, 2007) ("The court focused on the vast quantity of information a cell phone can store . . . "); State v. Smith, 920 N.E.2d 949, 954 (Ohio 2009) (objecting to the container analogy because of the cell phone’s inability to hold a tangible object).
\item \textsuperscript{86} United States v. Wurie, 728 F.3d 1, 6 (1st Cir. 2013) (citing Smallwood v. State, 113 So. 3d 724, 735 (Fla. 2013)).
\item \textsuperscript{88} Riley v. California, 134 S. Ct. 2473, 2480 (2014).
\item \textsuperscript{89} Id.
in its contents. Later, when back at the station, a detective who specialized in the gang examined the phone and purportedly found gang related photos and videos. This evidence was used to charge Riley for a gang shooting that occurred a few weeks prior to his arrest. During his trial, Riley moved to suppress the evidence found on his cell phone, claiming that the search violated his Fourth Amendment rights. The trial court denied his motion, and Riley was convicted on the shooting charges. His conviction was later affirmed at the appellate level. The California Supreme Court denied Riley’s petition for review and the Supreme Court of the United States granted certiorari.

In rendering its decision, the Supreme Court considered the facts in United States v. Wurie. In Wurie, an officer conducting routine surveillance witnessed what appeared to be a drug deal between two males in a vehicle parked in a nearby lot. He and a fellow officer later stopped one of the men and found two bags of crack cocaine. The man claimed he received the drugs from the other vehicle’s driver. A patrol car followed the other vehicle and subsequently arrested the driver, Wurie.

After bringing Wurie to the police station, the police found two cell phones and a set of keys, among other items. One of the cell phones rang several times with the caller I.D. screen reading “my house.” Officers opened the cell phone, saw a wallpaper picture of a woman with a small child, and pushed one button to access the call log. After accessing the call log, the officers pressed another button to reveal the number associated with the contact “my house.” An officer then ran the number through an online database, which gave the address for the number listed. The officers questioned Wurie about where he lived and Wurie denied living in the area with which the number was associated.

90. Id.
91. Id. at 2481.
92. Id.
93. Id.
95. Id.
96. Id.
97. See id. at 2481-82.
98. United States v. Wurie, 728 F.3d 1 (1st Cir. 2013).
99. Id.
100. Id.
101. Id. at 2.
102. Id.
103. Id.
104. United States v. Wurie, 728 F.3d 1, 2 (1st Cir. 2013).
105. Id.
106. Id.
107. Id.
Officers eventually took the keys and drove to the location where they thought Wurie lived under the belief that he was a drug dealer. When they arrived, they found a mailbox with his name on it and saw a woman and child who appeared to be the woman and child on the cell phone’s wallpaper. The officers searched the residence and discovered a large quantity of drugs, drug paraphernalia, guns, and ammunition. They charged Wurie with distribution of drugs, intent to distribute drugs, and with being a felon in possession of a firearm. Wurie filed a motion to suppress the evidence obtained as a result of the warrantless search of his cell phone, which was denied, and he was found guilty on all charges. On appeal, the First Circuit reversed the denial of Wurie’s motion to suppress, vacated his conviction, and remanded to the trial court. The Supreme Court granted certiorari.

In deciding Riley, the Supreme Court analyzed three separate precedents regarding searches of property around an arrestee. The three precedents include Chimel, Robinson, and Gant. The Court noted that Chimel introduced the “immediate control” standard, requiring that any property searched without a warrant must be located within the arrestee’s reach so as to create a threat of either harm to the officer or destruction of evidence. The Court interpreted Robinson, on the other hand, to say that the risks of concern in Chimel were assumed “present in all custodial arrests,” thus no case-by-case determination was necessary. Lastly, the Court examined Gant, which determined that warrantless searches of vehicles are only permissible if the arrestee is unsecured and within reaching distance of the area searched or if the officer has a reasonable belief that evidence of the crime for which the arrestee is being arrested might be located within the vehicle.

The Court reasoned that “[w]here a search is undertaken by law enforcement officials to discover evidence of criminal wrongdoing, . . . reasonableness generally requires the obtaining of a judicial warrant” and that, in the absence of a warrant, the search must fall within one of the recognized exceptions to the

---

108. Id.
109. Id.
110. United States v. Wurie, 728 F.3d 1, 2 (1st Cir. 2013).
111. Id.
112. Id.
113. Id. at 14.
115. Id. at 2483.
116. Id.
117. Id. See generally Chimel v. California 395 U.S. 752 (1969) (holding that searches incident to arrest must be limited to the area in the immediate control of the arrestee, and that the search must be justified in order to protect the officers or preserve evidence).
Fourth Amendment. The warrant system was put into place and is imperative to the legal system because it ensures that the decision of whether or not a search is reasonable and thus compliant with the Fourth Amendment is made by a detached and objective third party, such as a judge or magistrate, rather than by an officer in the heat of the moment.

The Court acknowledged that the word “exception,” in the context of the search-incident-to-arrest exception at least, is a “misnomer” because this purported exception occurs more frequently than searches pursuant to a warrant. The existing precedent is of little guidance when it comes to the expedited advancement of cell phone technology. The Court notes that it generally decides whether a particular search is exempt from the warrant requirement by using a balancing test, weighing “the degree to which it intrudes upon an individual’s privacy and . . . the degree to which it is needed for the promotion of legitimate governmental interests.”

The Court declined to follow Robinson because the facts present in Riley and Wurie did not support the need for a warrantless search. The interests outlined in Chimel were not in jeopardy to the extent that they were in Robinson and, further, a search of all of the data on one’s cell phone is much more invasive than a mere physical search of one’s person. The Court reasoned that while it is permissible for an officer to examine the phone’s physical exterior to ensure there are no immediate threats of harm, the digital information stored on the cell phone is not capable of physically harming anyone. The other interest identified in Chimel – that of preventing the evidence’s destruction – is likewise not preserved by allowing warrantless searches of cell phones incident to arrest. The United States and California, in these cases, have voiced concerns regarding the destruction of evidence through channels such as remote wiping or encryption; however, there is no evidence that these issues are prevalent or that allowing a search would alleviate that risk. Moreover, there are alternative ways for law enforcement to circumvent such issues by, for example, removing the phone from the network or placing the phone in bags that block radio waves and, in turn, the ability of a remote third party to “wipe,” or delete, the phone’s

121. Id. (quoting Johnson v. United States, 333 U.S. 10, 14 (1948)).
122. Id.
123. Id. at 2482 (quoting Wyoming v. Houghton, 526 U.S. 295, 300 (1999)).
124. See Riley, 134 S. Ct. at 2477.
126. Id. (The Court also noted that “[t]o the extent that a search of cell phone data might warn officers of an impending danger, e.g., that the arrestee’s confederates are headed to the scene, such a concern is better addressed through consideration of case-specific exceptions to the warrant requirement, such as exigent circumstances”).
127. Id. at 2479.
128. Id.
The Court further reasoned that if there are circumstances that plainly suggest that the phone is at risk of being remotely wiped, the officers may be able to conduct the search pursuant to the exigent circumstances exception. Therefore, under the facts of Riley and Wurie, allowing a warrantless search of a cell phone poses a greater threat to a person’s reasonable expectation of privacy than was present in the foregoing precedent.

The United States argued that past cases, which allowed various items including wallets and purses, are indistinguishable from Riley or Wurie and that, therefore, law enforcement should be permitted to search cell phones pursuant to the search-incident-to-arrest exception. The Court emphatically rejected that argument, stating that searches of digital information “implicate privacy concerns far beyond those implicated by the search of a cigarette pack, a wallet, or a purse.” The Court’s reasoning for this distinction was emphasized by the amount and variety of information that a cell phone holds.

While regular searches of an arrestee’s person or the area immediately surrounding him or her have physical limitations, those limitations do not protect searches of digital information on a cell phone. A standard smart phone has sixteen gigabytes of storage, which “translates to millions of pages of text, thousands of pictures, or hundreds of videos.” It is highly unlikely, if not impossible, that a comparable amount or variety of information could be obtained from a search of an arrestee’s person or the area within his or her immediate control. Additionally, the information stored on a cell phone can date back a significant period of time, keeping a digital record of one’s every move and thought. Thus, the Court held that cell phone searches are both quantitatively and qualitatively distinct from ordinary physical searches.

The Court found that the alternative proposals for how law enforcement should treat cell phones in the context of warrantless searches were either unclear or flawed. The Court’s primary objective in determining when application of the Fourth Amendment exceptions is appropriate is to provide clear and unambiguous guidelines for law enforcement. In order to maintain consistency and avoid law enforcement making every determination on an ad hoc basis, the Court ultimately decided that the Fourth Amendment’s search-incident-to-arrest

129. Id. at 2487.
130. Id. (citing Roaden v. Kentucky, 413 U. S. 496, 505 (1973)).
132. Id. at 2488 (citing United States v. Watson, 669 F.2d 1374, 1383 (11th Cir. 1982); United States v. Lee, 501 F.2d 890, 892 (D.C.C. 1974)).
133. Riley, 134 S. Ct. at 2488 (“That is like saying a ride on horseback is materially indistinguishable from a flight to the moon.”).
134. See id. at 2489.
135. Id.
136. Id.
138. Id. at 2491.
139. Id. at 2491-92.
exception does not justify the warrantless search of a cell phone, regardless of the circumstances. Cell phones are said to contain “the privacies of life,” and the balancing test used by the Supreme Court does not weigh in favor of infringing upon that privacy. The Court was careful to clarify that “the information on a cell phone is [not] immune from search,” but instead that “a warrant is generally required before such a search, even when a cell phone is seized incident to arrest.” The Court further explained that this ruling does not impede the government interests under the balancing test because law enforcement can obtain a warrant or, if the circumstances truly necessitate an immediate search, the exigent circumstances exception may apply.

IV. WARRANTS, SUBPOENAS, AND OTHER MEANS OF ACCESS TO DIGITAL INFORMATION

A. The Warrant Requirement

The Fourth Amendment provides that an individual’s right against unreasonable searches and seizures may not be violated unless a warrant is issued upon the showing of probable cause. In general, both the existence of probable cause and a valid warrant are required. Probable cause alone is insufficient to justify a warrantless search unless there are exigent circumstances that do not provide the officers with ample time to obtain a warrant. Prior to Riley, courts recognized that exigent circumstances existed where law enforcement unforeseeably discovered facts that provided probable cause and where (1) the evidence may have been destroyed or where the property was movable, (2) the person(s) subject to the search were alerted to the officers’ suspicions, and (3) when the contents may have never be found again if the officers had waited for a warrant. In the absence of such exigencies, courts have generally held that officers must obtain a warrant to perfect a valid search.

In order for law enforcement to obtain a warrant, a judge or magistrate must determine that the officers have probable cause that justifies the issuance of that

140. Id. at 2491-92, 2494-95.
141. Id. at 2494-95.
142. Id. at 2493.
144. U.S. CONST. amend. IV.
145. See id.
146. See generally Coolidge v. New Hampshire, 403 U.S. 443 (1971) (holding that the search of the accused’s vehicle was invalid because the officers had ample opportunity to obtain a warrant and no exigent circumstances existed).
148. Coolidge, 403 U.S. at 454-55 (noting that warrantless searches are per se unreasonable unless subject to an established exception and upon a showing that the exigencies made the search imperative).
warrant.\textsuperscript{149} The purpose of the probable cause standard is to ensure that the government is not permitted to search protected areas unless and until it has reason to believe that a specific crime has been or is being committed.\textsuperscript{150} As such, warrants tend to arise in the context of criminal law.\textsuperscript{151} While the definition of “probable cause” is somewhat uncertain, courts have found the term to mean “less than evidence which would justify condemnation”\textsuperscript{152} and have noted that a finding of probable cause may rest upon evidence that would not be competent at a criminal trial, meaning it falls short of the “beyond a reasonable doubt” standard.\textsuperscript{153} Instead, probable cause has been said to be more “akin to the more-likely-than-not standard.”\textsuperscript{154}

An officer that seeks a warrant must submit an affidavit stating the reasons for which he or she believes the search to be justified.\textsuperscript{155} If the facts set forth in the affidavit are such that a person of ordinary prudence would reasonably believe that offense did occur, then a warrant should be issued.\textsuperscript{156} In short, probable cause requires only a showing of the probability of criminal activity.\textsuperscript{157} Courts have held that showings that are “on the fence,” so to speak, should be decided in favor of issuing a warrant,\textsuperscript{158} and it is well-settled that the burden of making this showing rests on the government, i.e., the officer seeking the warrant.\textsuperscript{159}

\textbf{B. Subpoenas vs. Warrants}

Another avenue for obtaining information, aside from procuring a warrant and conducting a search, is to issue a subpoena. Unlike warrants, subpoenas are used both in criminal and civil contexts.\textsuperscript{160} Further, failure to respond to a criminal or civil subpoena may result in criminal consequences.\textsuperscript{161} A subpoena is “a formal demand for tangible items.”\textsuperscript{162} Subpoenas may be issued by the

\begin{itemize}
\item \textsuperscript{149} Jones v. United States, 357 U.S. 493, 498 (1958).
\item \textsuperscript{150} See Berger v. New York, 388 U.S. 41, 55 (1967) (citing Carroll v. United States, 267 U.S. 132, 162 (1925)).
\item \textsuperscript{151} See id.
\item \textsuperscript{152} United States v. Ventresca, 380 U.S. 102, 107 (1965) (quoting Locke v. United States, 11 U.S. 339, 348 (1813)).
\item \textsuperscript{153} See id. (citing Draper v. United States, 358 U.S. 307, 311 (1959)).
\item \textsuperscript{154} Christopher Slobogin, \textit{Subpoenas and Privacy}, 54 DEPAUL L. REV. 805, 807 (2005).
\item \textsuperscript{155} See Aderhold v. United States, 132 F.2d 858, 859 (5th Cir. 1943).
\item \textsuperscript{156} Id. (citing Stacey v. Emery, 97 U.S. 642 (1878); Carroll v. United States, 267 U.S. 132 (1925); Dumbra v. United States, 268 U.S. 435 (1925)).
\item \textsuperscript{157} United States v. New Jersey, 429 F.2d 950, 955 (3d Cir. 1970) (quoting Spinelli v. United States, 393 U.S. 410, 419 (1969)).
\item \textsuperscript{158} See id.
\item \textsuperscript{159} United States v. Rivera, 321 F.2d 704, 708 (2d Cir. 1963).
\item \textsuperscript{160} Rhonda Wasserman, \textit{The Subpoena Power: Pennoyer’s Last Vestige}, 74 MINN. L. REV. 37, 76-77 (1989).
\item \textsuperscript{161} Id. at 135 (discussing the results of failing to honor a subpoena, such as criminal contempt charges, fines, and imprisonment.).
\item \textsuperscript{162} Slobogin, supra note 154, at 805.
\end{itemize}
government, a government agency, or, in the case of a pseudo-subpoena, the average citizen. With merely a subpoena, the government may access a person’s medical, educational, and financial records.

Courts in the past have held that the only standard to which the government is held to in issuing a subpoena is that the information be “relevant to an investigation conducted for a ‘legitimate purpose.’” A subpoena’s recipient may challenge it prior to actually handing over any documents by claiming privilege, irrelevance, or that the demand is too burdensome. All three of these challenges, however, are rarely successful. Likewise, courts have held that a person cannot challenge a subpoena issued to a third party, such as a telephone company, on the grounds that it is a violation of his or her Fourth Amendment rights.

To that point, courts have generally rejected claims that subpoenas violate Fourth or Fifth Amendment rights for a number of reasons, including the contentions that subpoenas do not involve the same physical intrusion of a search and that applying stringent Fourth Amendment requirements to subpoenas would threaten investigations. Overall, there are very few regulations or requirements for the issuance of subpoenas as they seemingly require no actual evidence, resulting in the ease of access to a plethora of information.

C. Obtaining Information via Discovery

Parties to a case can also gain access to information by requesting the information during the discovery phase. Generally, the only requirement strictly enforced as to discovery requests is that the information requested be relevant to the case. Further, materials can be deemed relevant irrespective of whether they would be admissible at trial. Relevancy is broadly construed, and discovery requests should be deemed relevant if there is any possibility the

163. Id. at 806-07, 806 n.10.
164. Id. at 807.
165. Id. at 816 (quoting United States v. Powell, 397 U.S. 48, 57-58 (1964)).
166. Id. at 806.
167. Id.
168. Slobogin, supra note 154 at 823-24 (quoting United States v. Miller, 425 U.S. 435, 443 (1976) (the Court had “held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities.”)). See also Couch v. United States, 409 U.S. 322, 335 (1973) (“[T]here can be little expectation of privacy where records are handed to an accountant, knowing that mandatory disclosure of much of the information therein is required in an income tax return.”).
169. Id. at 809.
170. See id. at 844-45.
171. See id. (providing that the scope of discovery is consistent with Rule 26 (b)). See also Fed. R. Civ. P. 26(b) (“Parties may obtain discovery regarding any nonprivileged matter that is relevant to any party’s claim or defense—including the existence, description, nature, custody, condition, and location of any documents or other tangible things and the identity and location of persons who know of any discoverable matter.”).
information could be relevant to a claim or defense of any party.\textsuperscript{174} Similarly, courts have allowed the discovery of the same information in criminal cases as well.\textsuperscript{175} Due to Fourth and Fifth Amendment protections, however, discovery in criminal cases tends to be a bit more narrow.\textsuperscript{176}

V. THE EASE OF ACCESS TO DIGITAL INFORMATION STORED ON CELL PHONES

The government is able to obtain a substantial amount of information pursuant to a simple subpoena.\textsuperscript{177} In addition to medical, educational, and financial records, the government has access to stored emails, phone company records, internet provider logs, and social media information.\textsuperscript{178} Similarly, other information such as the phone numbers and email addresses contacted by an individual of interest may be obtained upon nothing more than a law enforcement officer’s statement that such information is relevant to an ongoing investigation through an administrative subpoena issued to the provider of the requested information.\textsuperscript{179} This information (phone records, emails, internet history, etc.) is largely the same information contained on cell phones that the Riley Court was so


\textsuperscript{175} See generally United States v. Nicholas, 594 F. Supp. 2d 1116 (C.D. Cal. 2008) (allowing the discovery of emails written between the CEO of a company and his wife on alleged conspiracy charges because the co-defendant was entitled to them in order to prepare his defense).


\textsuperscript{178} Slobogin, supra note 154, at 807 (citing 18 U.S.C. 2703(a), (b) (2000) (authorizing, under the Electronic Communications Privacy Act (ECPA), subpoenas for e-mail that has been sitting on a server for longer than 180 days without being opened and for e-mail that the recipient has accessed and stored on an outside server for any length of time). If the information is stored with a service not available to the general public (e.g., one run by an employer), then the ECPA does not apply and the government may obtain the stored information (content or identifying) simply upon a request. See id. 2703(a)(1)-(3). With respect to Internet Service Provider logs, see 18 U.S.C. 2703(c), (d) (authorizing access to these records if the government alleges that the records are “relevant and material to an ongoing criminal investigation”). See also generally Junichi P. Semitsu, From Facebook to Mug shot: How the Dearth of Social Networking Privacy Rights Revolutionized Online Government Surveillance, 31 PACE L. REV. 291 (2011) (discussing what information is available to government officials and upon what showing).

\textsuperscript{179} See Slobogin, supra note 154, at 807 (citing 18 U.S.C. 3123(a)(1) (2000) (requiring courts to issue an order authorizing the use of pen registers and trace devices when a federal government attorney or state law enforcement officer certifies that phone numbers or e-mail addresses are “relevant to an ongoing criminal investigation”); 5 U.S.C.A. 552a(b)(7) (West Supp. 2004) (permitting a law enforcement agency to obtain any federal agency record upon a written request by the head of the law enforcement entity)). See also David Kravets, We Don’t Need No Stinking Warrant: The Rise of the Administrative Subpoena, WIRED (Aug. 28, 2012, 6:00 A.M.), http://www.wired.com/2012/08/administrative-subpoenas/.
concerned with protecting. The Court in Riley determined that the appropriate solution was to require a warrant for any search incident to arrest unless the rare exigent circumstances exception applies. In doing so, the Court essentially required that law enforcement have probable cause to conduct searches of persons or property. This is a noble aspiration; however, the government is still able to obtain highly “personal, private information on a far lesser showing.”

The government’s access to this private information is nearly unlimited, with only a “federal official’s signature.” Congress has given this authority to a huge portion of the U.S. government as the federal official need not even be a judge. Administrative subpoenas have been used in a variety of investigations ranging from hazardous waste disposal to child exploitation to medical insurance fraud. Government officials have even been quoted as saying that they use administrative subpoenas presumeably because they have a “much, much lower threshold than a search warrant.” This raises substantial concerns as to the abuse of the subpoena process because there is essentially no oversight required.

A recent trend involves the use of administrative subpoenas in drug investigations, similar to the situation in Wurie. For example, the Drug Enforcement Agency (“DEA”), a government agency, starts with an informant or with the arrest of someone suspected of drug charges. From there, the DEA is able to use an administrative subpoena to access a log of all of the suspect’s incoming and outgoing calls, as well as message logs of all of the phone numbers associated with incoming and outgoing text messages. The DEA can then use that information to subpoena the same information from any or all of the numbers that they identify through the original subpoena, gaining access to the personal information of people whose names or associations they do not even know. In such a case, not only is there no probable cause, but the so-called

180. See Riley v. California, 134 S. Ct. 2473, 2489 (2014) (demonstrating concern over the privacy of the “millions of pages of text, thousands of pictures, or hundreds of videos” that cell phones contain).
181. Id. at 2493.
182. See Slobogin, supra note 154, at 807 (citing 3 WAYNE R. LAFAVE ET AL., Criminal Procedure § 135 (2d ed. 1999)) (“[T]he government usually needs probable cause - akin to a more-likely-than-not standard - to search ‘houses, persons, papers and effects.’”). See also u.S. Const. amend. IV (“[N]o [w]arrants shall issue, but upon probable cause”).
183. Slobogin, supra note 154, at 807.
184. Kravets, supra note 179.
185. Id.
186. Id.
187. Id.
188. See id.
189. See id.
190. Kravets, supra note 179.
191. Id.
192. Id.
“investigation” essentially becomes a fishing expedition into the records of individuals who have yet to be identified, much less suspected of a crime.\footnote{193}{See Slobogin, \textit{supra} note 154, at 807.}

Cell phone companies continue to be one of the biggest targets for subpoenas.\footnote{194}{See Kravets, \textit{supra} note 179.} In 2011, the nation’s mobile carriers collectively received over 1.3 million subpoena requests for subscriber information.\footnote{195}{Id.} AT&T, the nation’s second largest carrier, reported that the number of requests it received more than doubled between 2007 and 2011, totaling approximately 131,400 requests in 2011.\footnote{196}{Id.} Compare that number with the 49,700 court orders AT&T received in 2011, and it is evident that subpoenas are becoming quite the popular alternative to obtaining a court order or warrant through the court system.\footnote{197}{Id.}

This ease of access incites great suspicion as to whether lack of probable cause is simply an incidental by-product of the use of subpoenas or if government agencies use subpoenas precisely so that they might circumvent the probable cause standard guaranteed under the Fourth Amendment.\footnote{198}{Id.} Administrative subpoenas were not perceived as a threat to the Fourth Amendment initially because they were primarily sought in the business or corporate context, directing requests at companies suspected of criminal activity or regulatory non-compliance.\footnote{199}{See Slobogin, \textit{supra} note 154, at 811.} They were not seen as targeting individuals for their personal information.\footnote{200}{Kravets, \textit{supra} note 179.} Now, however, that is exactly what the administrative subpoena process aims to achieve.\footnote{201}{Id.} This problematic practice was foreseen and chastised nearly a century ago when Justice Holmes declared:

\begin{quote}
\[\text{[a]nyone who respects the spirit as well as the letter of the Fourth Amendment would be loath to believe that Congress intended to authorize one of its subordinate agencies to sweep all our traditions into the fire and to direct fishing expeditions into private papers on the possibility that they may disclose evidence of a crime.}\]
\end{quote}

Justice Holmes was not the last to recognize this injustice; however, those who have attempted to quash administrative subpoenas in court have been largely unsuccessful.\footnote{202}{Fed. Trade Comm’n v. Am. Tobacco Co., 264 U.S. 298, 305-06 (1924) (citing Interstate Commerce Comm’n v. Brimson, 154 U.S. 447, 449 (1924)).}

\begin{footnotes}
194. See Kravets, \textit{supra} note 179.
195. Id.
196. Id.
197. Id.
198. See Slobogin, \textit{supra} note 154, at 811.
199. Kravets, \textit{supra} note 179.
200. Id.
201. See id.
\end{footnotes}
VI. MOVING FORWARD IN THE AREA OF DEVICE SEARCHES AND OBTAINING DIGITAL INFORMATION

While the Riley decision’s impact on cell phones is evident, it is equally important to understand the implications the decision has on other forms of technology. What standards are currently required for the search of a computer, camera, or tablet, for example? The government cannot obtain all records held on a computer; however, other extremely broad requests have been upheld, such as “all records of gang-related activity” and “all records relating to violations of 21 U.S.C. 844.”204 The rule disallowing the search of everything on a computer is referred to as the “particularity rule.”205 Some suggest this rule has little meaning because, to even know such information is likely to exist on the computer – i.e., in order to reach the level of the probable cause requirement – the government must take at least a preliminary look at everything on the computer.206 This seems to only be of concern if probable cause is not established independent from the computer itself, in which case a warrant would probably not be issued in the first place.

In contrast, it is possible to isolate the information one wishes to search on a computer so as to not search so broadly that it violates Fourth Amendment particularity standards.207 Courts have been very lax on this standard however, and it is not uncommon for a court to allow a general search, notwithstanding any potential particularity issues.208 While there is little to no precedent regarding tablet devices, such as iPads, and how their searches are governed, courts have generally analogized them to a laptop computer, presumably making them subject to the same standards as computer searches.209 Information on searches of an arrestee’s camera is likewise scarce, but under the Riley reasoning, these searches should also be immune to Fourth Amendment exceptions.210

Regardless of whether the physical objects containing digital information are cell phones, computers, tablets, or cameras, the ease of access to the digital information they contain is still concerning with regard to the Fourth Amendment’s guarantee of privacy. There are a few differences in obtaining information through a device’s search and obtaining the same information

205. See id.
206. See id.
208. Id. at 1-2.
209. See United States v. Wurie, 728 F.3d 1, 3-4 (1st Cir. 2013).
210. See Riley v. California, 134 S. Ct. 2473, 2489 (2014) (finding that cell phones were not subject to the search-incident-to-arrest exception because the information stored on them cannot physically harm law enforcement officers, that there is generally little to no risk of the evidence on them being destroyed in the time it takes to obtain a warrant, and that they are distinct from other containers because of the amount and nature of the information they contain).
through a subpoena to a third-party provider, but none of them substantially alter the level of invasiveness.\textsuperscript{211} For example, there would be a slightly longer wait between the time of arrest and the time when law enforcement is able to view the information due to the time it would take for the officer or agency to draft and serve the subpoena and for the provider to gather and provide the information.\textsuperscript{212} This method would entail more work for the officer or agency to submit subpoenas to various providers, rather than to instantly have all of the information consolidated onto one device.

Despite these differences, however, the result is the same. The government is still able to obtain phone call logs, phone numbers associated with incoming and outgoing text messages, email addresses for incoming and outgoing emails, as well as the email subject lines, financial records, internet history, and possibly more, while avoiding the probable cause requirement.\textsuperscript{213} The availability of this information in a different form when obtained via subpoena does not render it any more or less worthy of privacy.\textsuperscript{214} The balancing test referenced by the Court in \textit{Riley} continues to be good law, and nothing in the Court’s decision gives the impression that the same digital information should be treated any differently when considered separate and apart from a device on which it may or may not be located.\textsuperscript{215}

\textbf{VII. Conclusion}

As indicated above, the use of technology continues to grow and expand almost daily. In order to achieve the Supreme Court’s purpose of consistency in instructing law enforcement as to what they can and cannot legally search, as well as its purpose of protecting the rights of individuals envisioned by the nation’s founders, it is vital that these issues are addressed as proactively as possible.\textsuperscript{216}

While the Court in \textit{Riley} had noble intentions and attempted to adequately preserve Fourth Amendment rights, its decision is futile unless and until more regulation and oversight is placed on the issuance of subpoenas, particularly the administrative subpoena. If the Supreme Court’s goal is to truly shield all of one’s private information that could be found on his or her cell phone under the probable cause standard, the only adequate solution is to eliminate administrative subpoenas altogether. This solution would be consistent with the \textit{Riley} decision because digital information is incapable of causing physical harm and is not

\textsuperscript{211} See Slobogin, \textit{supra} note 154, at 810-11.
\textsuperscript{212} See id.
\textsuperscript{213} See, e.g., id. at 807; Kravets, \textit{supra} note 179. See also Semitsu, \textit{supra} note 178.
\textsuperscript{214} See \textit{Riley}, 134 S. Ct. at 2495.
\textsuperscript{215} See generally id. at 2489 (holding that an individual’s right to privacy in regards to the contents of his or her cell phone outweigh any potential government interest in a warrantless search of the device).
\textsuperscript{216} See id. at 2491.
likely to be destroyed, especially when that information is stored by a third-party provider — law enforcement or any other government agency seeking the information should be required to obtain a valid search warrant.\footnote{217}{See id. at 2493.}

Additionally, a plain reading of the Fourth Amendment suggests that requiring anything less than probable cause would be a violation of the constitutional rights that U.S. citizens are all entitled to.\footnote{218}{See U.S. CONST. amend. IV.} The Fourth Amendment provides for the protection of ones “papers . . . against unreasonable searches and seizures” unless law enforcement obtains a valid warrant supported by probable cause.\footnote{219}{Id.} There is no reason why an individual should be afforded any lesser protection simply because the same information is contained in digital form, rather than on “paper.”\footnote{220}{See id. See also Riley v. California, 134 S. Ct. 2473, 2495 (2014) (“The fact that technology now allows an individual to carry such information in his hand does not make the information any less worthy of the protection for which the Founders fought”).} Abolishing the use of the administrative subpoena accomplishes this protection while remaining consistent with the Supreme Court’s guidance in Riley v. California.\footnote{221}{See generally Riley, 134 S. Ct. at 2473 (finding that the information found on one’s cell phone is deserving of protection from unreasonable searches).}
COBRA DATA AND THE RIGHT TO CONFRONT TECHNOLOGY AGAINST YOU

Kathleen E. Watson*

I. INTRODUCTION

Every state has implied consent statutes. Implied consent statutes provide that by simply driving in the state, the driver agrees to certain things. For example, many statutes provide that drivers implicitly agree to breath, blood, or urine testing upon an officer having probable cause to believe that the driver is impaired. While a driver has the physical ability to refuse such a test, that refusal comes subject to penalties and a record.

Additionally, every state has “per se” statutes that make it a crime to drive with a level of ethanol in the blood or breath that exceeds certain statutory limits, regardless of actual impairment. The trend of adopting per se statutes began

* J.D. candidate 2015 at the Salmon P. Chase College of Law at Northern Kentucky University.


3. Urine samples are the least reliable of the three types of chemical tests available and in some states urine testing is unavailable for DUI. See The Role of Biomarkers in the Treatment of Alcohol Use Disorders, SUBSTANCE ABUSE AND MENTAL HEALTH SERV. ADMIN. (2006), available at http://www.samhsa.gov/SAMHSA_News/VolumeXIV_6/article5.htm (stating that urine testing is too sensitive and prone to delivering false positives).

4. See, e.g., Summers v. Utah, 927 F.2d 1165 (10th Cir. 1991) (finding probable cause to arrest for DUI when officer detected scent of alcohol on the driver and the driver refused to perform a field sobriety test); Miller v. Harget, 458 F.3d 1251 (11th Cir. 2006) (finding probable cause to arrest for DUI when officer smelled alcohol from the vehicle’s interior and the driver refused to take a breathalyzer test); Kinlin v. Kline, 749 F.3d 573 (6th Cir. 2014) (finding probable cause to arrest for DUI when officer detected scent of alcohol on the driver, the driver admitted to drinking two beers and refused to take any field sobriety tests).

5. Generally, states provide for breath, blood, or urine testing. See generally 8 AM. JUR. 2D Automobiles § 991 (2014). In most DUI cases, California provides for breath or blood testing only. CAL. VEH. CODE ANN. § 23612 (West 2014). In some states the officer making the arrest gets to choose the type of chemical test to be offered. See, e.g., ARK. CODE ANN. § 5-65-203(b)(1) (West 2014); TENN. CODE ANN. 55-10-406 (West 2014).

6. Most states have enacted a statute criminalizing the refusal to submit to chemical testing as a separate and distinct offense from the related traffic or DUI offense. Penalties include a wide range of license suspensions, jail sentences, and fines. See, e.g., OHIO REV. CODE ANN. § 4511.191 (West 2014); KY. REV. STAT. ANN. § 189A.105 (West 2014); see generally FLEM K. WHITED, III, DRINKING/DRIVING LITIGATION: CRIMINAL AND CIVIL § 11:16 (2d ed. 2014).

7. See generally, 1 RICHARD E. ERWIN, DEFENSE OF DRUNK DRIVING CASES: CRIMINAL, CIVIL § 1.05(1)(a) (Matthew Bender, 3d ed. 1975).
after Congress conditioned the availability of federal highway funds on a state’s adoption of a 0.08% blood alcohol concentration (BAC) limit in 2004.\(^8\)

The advent of ‘per se’ statutory provisions placed an increased burden on the science of breath testing, because the testing of breath in the previous statutory scheme permitted a defendant to argue that despite an alcohol level that exceeded .08, that in fact they were not impaired. Under the new statutory scheme, that defense is no longer available.”\(^9\)

Under this new scheme, a breath test result may be the only evidence against an accused, and still be enough evidence to convict.\(^10\) Together, these statutes provide that a driver must give the state what could be prima facie evidence of guilt. Thus, the accuracy and reliability of breath tests are imperative.

“The Confrontation Clause applies to technological scientific testing and in a DUI breath test case, the defendant has the right to receive full information regarding the test and testing device used as the basis for the allegation.”\(^11\)

Computer On-Line Breath Records Archive (COBRA) data contains a multitude of information regarding particular breath testing devices and breath tests given; the information is stored in a centralized database maintained by the state, and is easily accessible.\(^12\) “Confronting database output means questioning the entire system: data collection, entry, storage, retrieval, analysis and production.”\(^13\)

Part II of this article begins with a discussion of the right to confrontation and how advancement in technology has impacted that right. Part III includes an overview of the potential exculpatory value of COBRA data\(^14\) and examines the various state approaches to determining whether the defendant has a right to such information, including the recent Ohio Supreme Court decision in Cincinnati v. Ilg. Part III concludes with a comparison of the DUI breath test defendant’s right to COBRA data with decisions regarding discovery of similar databases and similar technology. “The objective of the defense is to discredit, whenever possible, the accuracy of a breath alcohol machine through discovery . . . .”\(^15\) To ensure a DUI breath test defendant’s rights to confrontation and a fair trial, COBRA data must be discoverable.

---

8. Id. at n. 4.
10. Some scholars argue that per se statutes essentially create a “presumption of guilt” based on a test result. See, e.g., id. at 427 (“Clearly a ‘presumption of guilt’ based on a test result neutralizes the ‘presumption of innocence’ believed to be a well-settled part of American jurisprudence.”).
12. See infra text accompanying notes 48-49.
14. COBRA, meaning “Computerized Online Breath Records Archives.”
15. Sapir & Giangrande, supra note 11, at 25.
II. THE RIGHT TO CONFRONT WITNESSES AGAINST YOU

The Sixth Amendment to the U.S. Constitution guarantees that “in all criminal prosecutions, the accused shall enjoy the right . . . to be confronted with the witnesses against him . . . .”\(^{16}\) The right is both fundamental and essential for the protection of life and liberty.\(^{17}\) “The central concern of the Confrontation Clause is to ensure the reliability of the evidence against a criminal defendant by subjecting it to rigorous testing in the context of an adversary proceeding before the trier of fact.”\(^{18}\) Thus, the right is not limited to confronting persons, but rather it encompasses the right to confront evidence in general.\(^{19}\) Without the opportunity to confront prejudicial evidence, the accused cannot have a fair trial.\(^{20}\)

Throughout the nineteenth and twentieth centuries, courts were addressing Sixth Amendment issues regarding what constitutes evidence against an accused and under what circumstances the right to confront that evidence is subject to exception.\(^{21}\) However, the same issues have continued to resurface throughout the twenty-first century as a result of advancements in technology that have altered our understanding of evidence and cross-examination.\(^{22}\)

A. History of the Right

The right of confrontation is based on a theory of natural justice that demands opportunity for cross-examination.\(^{23}\) The right is not subject to any new exceptions.\(^{24}\) However, the Supreme Court in *Crawford v. Washington* held that

---

16. *U.S. Const.* amend. VI.
20. *Alford v. United States*, 282 U.S. 687, 692 (1931); *see also Pointer v. Texas* 380 U.S. 400, 404 (1965) (“[T]o deprive an accused of the right to cross-examine the witnesses against him is a denial of the Fourteenth Amendment’s guarantee of due process of law.”).
21. *See, e.g.*, *Coy v. Iowa*, 487 U.S. 1012, 1017 (1988) (“There is something deep in human nature that regards face-to-face confrontation between accused and accuser as ‘essential to a fair trial in a criminal prosecution.’”) (*quoting Pointer*, 380 U.S. at 404); *Ohio v. Roberts*, 448 U.S. 56, 65 (1980) (holding that an unavailable witness’s testimony is admissible when the witness is unavailable at trial and the testimony has indicia of reliability).
22. Courts now recognize exceptions to the defendant’s right to face-to-face confrontation. *See, e.g.*, *United States v. Brown*, 528 F.3d 1030 (8th Cir. 2008) (allowing child abuse victim to testify via closed circuit television); *Kramer v. State*, 277 P.3d 88 (Wyo. 2012) (allowing a witness to testify via video conference when necessary to further an important public policy and the reliability of the testimony is otherwise assured).
24. *Crawford v. Washington*, 541 U.S. 35, 54 (2004) (citing *Mattox v. United States*, 156 U.S. 237, 243 (1895)) (“The text of the Sixth Amendment does not suggest any open-ended exceptions from the confrontation requirement to be developed by the courts. Rather, the ‘right . . . to be confronted with the witnesses against him,’ is most naturally read as a reference to the right of confrontation at common law, admitting only those exceptions established at the time of the founding.”). *Crawford*, 451 U.S. at 57-61 (noting the exception that testimonial hearsay may be
the right applies to “testimonial statements.”

A testimonial statement is “[a] solemn declaration or affirmation made for the purpose of establishing or proving some fact.”

Documents that are prepared in anticipation of litigation are testimonial. For example, the Supreme Court held in Melendez-Diaz, that a forensic analysis certificate, confirming that a certain substance is a narcotic, is a testimonial statement.

In Bullcoming v. New Mexico, the Supreme Court, relying on its reasoning in Melendez-Diaz, held that a blood alcohol test result is a testimonial statement. Despite the state’s argument that the analysis was not “adversarial” or “inquisitorial,” but rather an observation of an “independent scientist” made according to a “non-adversarial public duty,” the Court held that a document created solely for an evidentiary purpose made in aid of police investigation is clearly testimonial.

Likewise, a breath test is given for the purpose of detecting a prohibited level of breath alcohol and prosecuting impaired driving. A breath test result is a document created for evidentiary purposes in aid of police investigation and used to establish the amount of alcohol in a person’s system. In this regard, a breath test would also appear subject to confrontation. However, several courts have held breath test results non-testimonial as the test results are documents created by a machine rather than a statement or certification made by a human analyst.

Even so, in the case of per se charges, the state’s reliance on a breath test results includes testimony that the breath testing machine used was accurate and reliable at the time the test was given and that the testing procedure used was adequate to ensure an accurate result. “The breath test result is only as reliable as the machine, the operator, and the procedures followed.” Thus, the accused has the right to confront such evidence through cross-examination of the officer who administered the test, the senior breath test machine operator and, when given access to the necessary documentation regarding how the machine is functioning, through testimony of a defense expert witness.

used against the accused when the declarant is unavailable and the defendant has had the opportunity to cross-examine the declarant).

26. Id. at 51.
28. Id.
30. Id.
32. Sapir & Giangrande, supra note 11, at 8; see also In re Winship, 397 U.S. 358, 363-64 (1970) (Due process prohibits conviction of an individual for a criminal offense, except upon proof of guilt beyond a reasonable doubt for each element of the alleged crime.).
33. Sapir & Giangrande, supra note 11, at 19.
B. The Impact of Technology

The advent of new technologies has impacted the Supreme Court’s interpretation of the Confrontation Clause.\textsuperscript{34} For example, face-to-face confrontation is no longer mandatory, but preferable. Nowadays, remote testimony in pretrial hearings is routine. Some states have even enacted statutes that allow laboratory analysts to testify at trial via technological means.\textsuperscript{35}

Predating remote testimony, yet continuing to show up time after time in Sixth Amendment litigation, are issues regarding access to government-controlled databases.\textsuperscript{36} “Increasingly, both sides are looking toward nonhuman sources of information in preparing their cases. Databases in a raw sense are an extension of human memory and computational ability. It is only natural that they have become powerful and increasingly common witnesses in many prosecutions.”\textsuperscript{37} Databases are exceptional in that the information capable of being input is unlimited. Additionally, databases include both technological and human components, thus subjecting the accuracy and reliability of results to human error. “[E]lectronically collected information sources are a double-edged sword. Their accuracy and reliability are critical issues in the hands of prosecutors and their accessibility a hard-won necessity in preparing a defense.”\textsuperscript{38}

Like breath test results, DNA is also a type of evidence that alone has the ability to convict.\textsuperscript{39} As such, courts have begun recognizing the defendant’s right to access DNA databases.\textsuperscript{40} Both state\textsuperscript{41} and federal\textsuperscript{42} legislatures have also recognized the potential exculpatory value of DNA databases and provided defendants with a statutory right to that information under certain circumstances.

The new technology age has drastically altered the type of evidence commonly used to convict. Things like the amount of evidence, corroborating circumstances, and credibility of lay witness testimony have all lost importance in the face of technical evidence. The state relies on the accuracy and reliability

\begin{thebibliography}{9}
\bibitem{35} \textit{See, e.g.}, ARK. CODE ANN. 12-12-313(e) (West 2014); KAN. STAT. ANN. 22-3437(b) (West 2014).
\bibitem{36} \textit{See infra} text accompanying notes 107-119.
\bibitem{37} Strutin, \textit{supra} note 13, at 9.
\bibitem{38} \textit{Id.} at ¶1.
\bibitem{40} \textit{See generally} Strutin, \textit{supra} note 13.
\bibitem{42} \textit{See} Justice For All Act of 2004, Pub. L. No. 108-405, 118 Stat. 2260 (codified as amended in scattered sections of 18 U.S.C. & 42 U.S.C.). The Innocence Protection Act provides federal prisoners with a right to DNA testing, provides incentive grants to states to implement reasonable measures to preserve biological evidence, and provides post conviction access to testing. \textit{Id.}.
\end{thebibliography}
of technical evidence to convict. To present a credible defense, the accused must call into question the accuracy and reliability of the technical evidence against him.

In the case of breath testing, the legislature gives technical evidence a statutory presumption of accuracy and reliability in order to guarantee its admittance, thus limiting pretrial attacks on admissibility and leaving the accused to convince the trier of fact not to give much weight to the scientific evidence at trial. COBRA data can provide reasonable doubt as to the validity of a breath test result.

III. COBRA DATA

Evidentiary breath testing machines are “machines whose results are generally admissible at trial.”\(^43\) There are four manufacturers of these machines in the United States: CMI, Draeger, Intoximeters, and National Patent.\(^44\) Breath testing devices collect a great deal of information regarding the particular machine and the tests given on that machine.

Some portion of that information is recorded on paper, and some of the information is recorded in the machine. The information recorded in the machine is often referred to as the “vital” data for the testing process. That vital data is electronically transmitted to a centralized computer that is usually located at the jurisdiction’s agency headquarters. Centrally managed data is generically referred to as ‘COBRA data’, named after the application program sold by CMI which collects and manages data for breath tests performed by Intoxilyzer models built and sold by CMI.\(^45\)

Likewise, this paper uses the term “COBRA data” to refer to any and all information recorded by evidentiary breath testing machines and processed by applicable data management programs.

COBRA data contains approximately 60 Excel-like tables of information specific to each breath testing machine.\(^46\) The information includes things like: atmospheric pressure, tank pressure, subject breath volume, flow rate, sample chamber temperature, breath sample temperature, sample attempts, sample duration, remote calibration, remote maintenance, direct calibrations, direct calibrations, and more.

---

43. As opposed to preliminary breath testing machines whose results are generally not admissible in evidence. See Thomas E. Workman, Jr., The Science Behind Breath Testing for Ethanol, 7 U. MASS. L. REV. 110, 116 (2012).
44. Id. at 114.
45. Workman, Jr., supra note 9, at 226.
maintenance, parts replacements, error records, diagnostic records, and subject test records.47

All of the information recorded is machine specific and the central database can be searched using a machine’s serial number.48 Searching the information and copying it to a disc takes less than 10 minutes and the only cost involved is that of the disc being used.49 Thus, to comply with a discovery request, the state can easily find and produce the requested information for negligible cost.

The most important issue arising out of the chemical test program employing breath methods of analysis is raised by lay people who have no knowledge or experience in this field, but a basic right to question. Lawyers are obligated by their professional integrity to establish the validity of any given breath test for alcohol when the results of such test are to be used as evidence against a client they are representing. This must and should be accomplished by diligent searching interrogation.50

In some cases the defense may be able to offer evidence of an accused’s sobriety to rebut evidence of impairment. In the case of per se charges, however, evidence of sobriety will not likely be enough to overcome the influence of a breath test result. In order to produce reasonable doubt as to the validity of a breath test result, the defense expert witness must have access to COBRA data. Without it, interrogation and cross-examination regarding the accuracy and reliability of a specific breath test is exceedingly limited.

A. Exculpatory Value

Breath testing machines are “electronic devices, controlled by a microprocessor and utilize complex software programs to interpret readings. They use electrochemical fuel cells or infrared measurement of breath samples to calculate the amount of ethanol in the breath subject’s breath.”51 The science behind breath testing is subject to extensive criticism among experts.52 Each component of the scientific process is subject to vigorous debate regarding accuracy and reliability.53 While these broad theories of fallibility, margins of error, and potential for operator manipulation may be explained, COBRA data

48. THE OHIO CHANNEL, supra note 46.
49. Id.
50. Sapir & Giangrande, supra note 9, at 3.
51. Workman, Jr., supra note 43, at 116 (citing JAMES C. GARRIOTT, GARRIOTT’S MEDICO LEGAL ASPECTS OF ALCOHOL 401 (5th ed. 2008)).
52. See generally 70 AM. JUR. Trials (1999).
53. Id.
can reveal that those theories are in fact actualities, with regards to a particular machine at a particular time.

In 2008, a Florida study revealed that one in four breath tests administered with the Intoxilyzer 8000 did not report a numeric result. The same study revealed that one citizen was asked to give thirteen different breath samples in one hour because the breath testing machine was continuously registering errors. The Florida study was done using COBRA data, which includes records of troubleshooting information for each intoxilyzer machine. In Florida, COBRA data is made publicly available. This type of troubleshooting information, which directly relates to a specific machine’s accuracy and reliability, would never have been discovered without the use of COBRA data.

The defense must be given the opportunity to present evidence that establishes reasonable doubt. The Florida study is one example of how COBRA data can be used to create reasonable doubt as to the validity of a breath test result. A defendant’s Sixth Amendment right to confront the evidence against him should include the ability to present direct evidence that the breath testing machine registered errors 12 out of the 13 times it was used to test the defendant.

COBRA data can monitor an operator’s administration of the breath test. If a breath test is administered incorrectly, the results may be invalid. For example, breath tests require a certain air flow and volume to produce an accurate result. Thus, the administrator must counsel the subject on how long to blow into the device. The longer or hard a subject blows, the higher the test result may be. If a subject stops blowing before an adequate volume of air is supplied, the device may register a “refusal” or an incorrect numerical result. Additionally, an operator may be able to generate a refusal “at will” with certain types of breath testing machines. With the availability of COBRA data, some courts have found that the degree of possible operator manipulation required suppression of the results.

While there is much debate among scholars regarding proper administrative procedure, state agencies do at least set certain minimal administrative

54. Workman, Jr., supra note 9, at 211 (citing Public Records, Florida Department of Law Enforcement, available at http://www.webcitation.org/5YDIXsW6B).
56. Id.
58. See generally Michael C. Tilotson & Jeff Martin, VA. PRAC., VIRGINIA DUI LAW: UNDERSTANDING THE SCIENTIFIC, TECHNOLOGICAL, AND LEGAL ASPECTS OF A DUI CASE § 5:13 (West 2013-2014) (discussing how a suspect blows makes a difference in the test result).
59. Workman, Jr., supra note 9, at 213.
60. See id.
61. With the Draeger Alcotest 7110 MK III-C, pressing the start button during a test records a refusal. Workman, Jr., supra note 9, at 214.
62. Id. at 215 (citing State v. Briggs, 14 Fla. L. Weekly 973b, (Fla. Cir. Ct. 2007).
requirements and procedures, as evidenced in their operator manuals and training programs. If the state administrative requirements are not met, the defense can challenge the admissibility of the results. Even if the state’s administrative requirements are met, the defense can use expert testimony regarding the administration to convince a jury of the proper weight to give a test result. Similarly, COBRA data can also reveal patterns in breath tests over a period of time that evidence consistent administrator error.

Operator certification goes hand-in-hand with administration. State statutes require that officers who administer breath tests go through periodic certification. States differ on how often administrators must be re-certified, but all states require it. Generally, to be certified an officer is required to attend a continuing education course taught by a state agency on how to properly administer a test. COBRA data keeps track of which officer administers each test and whether the officer is currently certified to administer the test. In 2011, a Louisville, KY news source reported that several of the Louisville Corrections Officers failed to get the necessary re-certification, putting over 500 test results into question.

COBRA data can also keep track of the type and frequency of machine calibrations. Improper calibration will cause improper breath test readings and even properly calibrated machines will drift away from accuracy over time. For this reason, each state requires periodic calibration checks. A calibration check ensures that the testing device is properly measuring samples. In the event that a device gives results outside of the accepted range, there should be documentation explaining what was done to repair the problem.

“In June of 2010, The Washington Post reported that hundreds of defendants in the District of Columbia were wrongfully convicted of DUI because ‘the District’s badly calibrated equipment would show a driver’s blood-alcohol content to be about 20 percent higher than it actually was.’” Many states require suppression of a breath test result if the agency did not comply with the required calibration checks. Some states also require suppression if there is no documentation as to how an improper calibration check was remedied. While the state may be required to provide information regarding calibration in discovery per statutory requirements, most statutes only require calibration

---

66. Id. at 4 (citing Mary Pat Flaherty, 400 Drunken-Driving Convictions in D.C. Based on Flawed Test, Official Says, THE WASH. POST (June 10, 2010), http://www.washingtonpost.com/wpdyn/content/article/2010/06/09/AR2010060906257.html.).
records be kept for a limited period of time. COBRA data, on the other hand, can provide calibration records for a longer period of time, thus allowing an expert to examine possible trends in the particular machine’s need for regular calibration.

COBRA data includes records of when a specific machine is in and out of service, thus indicating when maintenance might have been done to the machine. Maintenance records are important for determining whether a specific device was working properly on a given day.69 The number of times that parts in a particular machine are repaired or replaced can shed light on the accuracy and reliability of the machine at a given time.70 Maintenance records can also reveal whether manufacturer recalls were complied with.

Additionally, maintenance records can be used to ensure that calibration checks were conducted after a parts replacement or repair, to make sure the device was reporting results within an acceptable range after repairs. Likewise, if there was no “taken out of service” notice or repair record when the machine was sent in for re-calibration, the defense can point out to a jury that there is no record of what problem the machine was having or if the problem was actually fixed.71

Operational malfunctions, like the 12 errors mentioned in the Florida case above, are generally considered malfunctions that are self-diagnosed and self-reported, meaning the administrator will immediately receive the error message on the device. COBRA data includes records and information about each time a malfunction is reported. Operational malfunctions can shed light on the inaccuracy and unreliability of the particular machine at a particular time. Operational malfunctions can include:

- **RFI Detected**: Self reporting of RFI indicates that Radio Frequency Interference has been detected by the machine. RFI can be self generated by components that are failing within the machine, or they can be the result of electronic equipment, which includes cell phones, police radios, air conditioners, refrigerators, computer printers, fluorescent lights, or virtually anything that either plugs in or has a battery.

- **Tolerance Failure**: The calibration sample supplied to the machine with a known amount of alcohol does not compute a value that is within the accepted tolerance.

- **Purge Fail**: The machine was unable to remove all of the ethanol from the chamber by blowing fresh air through the machine.

- **Interference Detected**: The machine has detected the presence of some material that distorts the ability to measure the subject’s breath.

70. Sapir & Giangrande, supra note 11, at 27.
• **Ambient Failure:** The machine is unable to calibrate itself based on the initial evaluation of the chamber of air before the test begins.

• **No .02 Agreement:** The samples supplied by the subject produce results that are more than .02 apart, which indicates that the machine is not able to measure the samples correctly.

• **Slope:** The machine is unable to calculate a result because the sensors vary more than a predetermined amount during the course of measuring 120 values per second over the course of a breath sample.

• **Diagnostic Failure:** The self diagnostic that is performed at the beginning or end of the test has determined that some aspect of the machine is not functioning correctly.

• **Range Exceeded:** The amount of measured alcohol exceeds .500, and it is presumed that the machine is not working correctly.  

It is important to point out that even with self-diagnosed, self-reported malfunctions, there is still controversy in the scholarly community as to whether the malfunction programming itself is accurate and reliable. In other words, even if the operational malfunctions are reporting as programmed, the program itself may be flawed or limited.

For example, antennas that measure RFI are usually directional and sensitive to a specific frequency range. In these instances, “RFI detected” will not report on the machine unless the frequency is coming from a certain direction and is within a certain frequency range. If COBRA data shows “RFI detected” malfunctions before or after a test that is used as evidence of impairment, there is a likelihood that interference still affected the test results, even though the machine did self-diagnose the problem. Cross-examination of the officer administering the test that shows the officer did not know where the interference was coming from might serve as corroborating evidence that the test results may have been affected. Interference can come from just about any electronic device and if RFI is not detected, “[s]uch interference can cause sensors to deliver a heightened voltage or current, inflating the readings of sensors in the machine.”

“A complete, documented, historical perspective on the individual breath alcohol machine, from the date of manufacture to the date of trial, is necessary for insight into the care, maintenance, repairs, testing, upgrades, recall compliance, use, problems, etc., of each unit.”  

This is precisely the reason that COBRA data must be discoverable. Any and all information relating to the accuracy and reliability of a specific breath testing instrument and breath test result should be available for cross-examination.

---

72. Workman, Jr., supra note 9, at 215-16.
74. Sapir & Giangrande, supra note 11, at 29.
B. Various State Approaches to Discovery

In *Hawaii v. Hsu*, the court declined to find a due process violation when COBRA data was not provided in discovery.\(^{75}\) The court found that the non-disclosure did not rise to the level of fundamental unfairness as the defense presented no evidence that the requested material would be exculpatory, but only that the material had the potential to be exculpatory.\(^{76}\)

In Florida,\(^{77}\) Washington,\(^{78}\) and South Carolina,\(^{79}\) all breath testing information is regularly published and made available to the public. The New Jersey Supreme Court has ordered the state to maintain a regularly-updated central database and provide defendants access to that database.\(^{80}\) Ohio currently has a database that is available online,\(^{81}\) however, this database contains only a small portion of the COBRA data that exists in the centralized database.\(^{82}\)

Most states have not so willingly provided the information. In *State ex rel. Games-Neely v. Overington*, the West Virginia trial court ordered the state to produce the downloaded data.\(^{83}\) The state filed a writ of prohibition to keep the judge from enforcing the order. At the hearing, the defense explained their data request:

[I]t’s a procedural history of the machine where you get to take a meaningful look at the calibration and how they’re doing it. How they’re doing their accuracy inspections, when they’ve exchanged their dry gas tanks. Every aspect that goes into it so when they hand you that printer ticket and say “trust us” you get a scrutinized and meaningful review of the most critical piece of evidence in a DUI case which is the breath box and the days of just handing them the ticket and say “trust us, that’s reliable” are over.\(^{84}\)

---

76. Id. at 11.
82. See State v. Muchmore, No. C-120830, 2013 WL 6118305, at *5 (Ohio Ct. App. Nov. 20, 2013). See also DUI Undo Consultants, supra note 47 (“When the defense bar in Ohio started challenging the reported BrAC results because of the “Fatal Flaw” in ‘Sample Attempts’ line of data what did the state of Ohio do? They removed the ‘Sample Duration & Sample Attempts’ data. . . . When Ms. Martin [Program Administrator with the State’s Alcohol and Drug Testing division in the Department of Health] was confronted about the ‘missing’ technical data, she clarified her statement in an email, admitting technical data was stricken . . .”).
84. Id. at 431–32.
The data request covered a time period from January 1, 2010 through March 1, 2011. The defense specifically addressed the need for data over the period of time:

[T]o fairly evaluate an evidential breath alcohol machine’s performance, it is necessary to have data from a year prior to the date of a defendant’s testing and a year subsequent, if possible. This wide time frame allows for a thorough review of how the instrument was functioning at a point in time pre or post the Defendant’s test in order to assess whether or not anything has changed with the instrument’s functionality. According to the Defendant, issues such as calibration stability and/or drift can only be evaluated if there is sufficient verification data, which is why the Defendant requires a wider window of operational data.

In affirming the circuit court’s decision, the West Virginia Court of Appeals agreed that the data request was both material and relevant. Even more, the court agreed that the defense has a “constitutional due process right to discover and to examine evidence that would tend to exculpate him. . . .”

Other state courts have required the production of COBRA data as well. In State v. Marino, a North Carolina trial court ordered the state to provide all of the downloaded data in its possession that was generated from the specific breath testing machine. In State v. Powers, a Wisconsin trial court held that the defendant was entitled to challenge the reliability of the breath test results through examination of the database involved. In Cincinnati v. Ilg, an Ohio trial court suppressed the defendant’s breath test results after the state refused to comply with a court order to produce the data. An Ohio appeals court upheld the decision and on June 11, 2014 the Ohio Supreme Court heard oral arguments. While the issue on appeal was whether the trial judge abused his discretion in suppressing the test results as a remedy to discovery violations, the oral arguments focused on whether the request for COBRA data was a valid discovery request. Ohio will be the first state supreme court to address the issue.
C. Cincinnati v. Ilg

In Ilg, the state argued that an earlier Ohio Supreme Court case, State v. Vega, made COBRA data irrelevant and thus not subject to discovery. Vega specifically held that the defense cannot challenge the general accuracy and reliability of the science behind breath testing machines and administrative procedures that have been approved by the Ohio legislature or the Ohio Department of Health. Accordingly, the state argued that because the breath testing machine and procedures used to test Mr. Ilg were approved by the legislature, the accuracy and reliability of the testing machine and testing procedures could not be attacked, thus making COBRA data irrelevant.

The defense responded that the discovery request was not to challenge the general reliability of the legislature-approved machine and procedures, but rather that the data requested was specific to the intoxilyzer machine used on the defendant, and the purpose of requesting the information was to prepare for cross-examining the accuracy and reliability of the specific intoxilyzer on the day that it was used to test the defendant and the administration of the defendant’s test. The defense argued that COBRA data could reveal problems with the specific intoxilyer, without attacking the general reliability of the machine model or the science behind breath testing.

Vega recognized that the statutory presumption of validity for approved machines and administrative techniques is rebuttable. “The defendant may still, notwithstanding the presumption, establish if he can that he was not under the influence of alcohol at the time of his arrest or that there was something wrong with the test and the results were erroneous.” The court further noted that rebuttable evidence might include non-technical evidence or technical evidence and expert testimony. In Ilg, the Ohio Supreme Court recognized this language from the Vega decision and the defendant’s right to confront a breath test result, despite the statutory presumption of validity. Accordingly, Ilg upheld Vega’s prohibition that the defendant may not attack the general reliability of approved breath testing machines and administration, but recognized that the defendant

* The author wishes to extend her sincerest thanks and appreciation to Mr. Ilg’s defense attorney, Steve Adams of The Law Office of Steven R. Adams, for the clerking experience and exposure, which led to the publication of this note.

93. THE OHIO CHANNEL, supra note 46.
94. The COBRA data request was for information from a specific intoxilyzer, identified by serial number. Id.
95. Id.
96. Id.
must have the right to attack the specific reliability and accuracy of the machine and administration used against the defendant.\textsuperscript{101}

The purpose behind the Ohio statute was to create a presumption of validity with chemical test results as to eliminate the state’s need for expert testimony establishing the accuracy and reliability necessary for admissibility of the test results.\textsuperscript{102} While discovery rules are generally state-specific, legislative presumptions regarding admissibility of chemical test results, like that at issue in \textit{Vega},\textsuperscript{103} are found in most states.\textsuperscript{104} The Ohio Supreme Court’s decision in \textit{Ilg} can serve as important persuasive authority that legislative presumptions of validity cannot prohibit the defendant from exercising his constitutional right to cross-examine the evidence against him and for purposes of trial, these statutes simply create a rebuttable presumption of validity, while allowing the jury to decide how to weigh the evidence.\textsuperscript{105} Most importantly, \textit{Ilg} recognized that a breath test defendant cannot challenge a breath test result without COBRA data.\textsuperscript{106}

\textit{Ilg}’s recognition of a breath test defendant’s right to COBRA data is likely to be the first step in addressing a multitude of related hurdles that a breath test defendant may run into in obtaining such data. These hurdles include that not all states require software programs like COBRA be purchased and used with breath testing machines. Some states may not even require the use of machines that are compatible with such programs. Additionally, some programs may not be as user-friendly or keep track of as much information as that of the COBRA program compatible with the Intoxilyzer 8000.

\section*{C. Similar Issues with Similar Technology}

From a broader perspective, the issue is one of defense access to government databases. Courts have recognized the exculpatory value of questioning the

\textsuperscript{101} \textit{Id.} at 285.
\textsuperscript{102} \textit{Vega}, 465 N.E.2d at 1307.
\textsuperscript{103} \textit{O.H. REV. CODE ANN.} § 4511.19 (West 2014) (“In any criminal prosecution for a violation of this section . . . the court may admit evidence on the concentration of alcohol in the defendant’s blood at the time of the alleged violation as shown by chemical analysis of the defendant’s . . . breath . . . withdrawn within two hours of the time of such alleged violation. . . . Such bodily substance shall be analyzed in accordance with methods approved by the director of health, by an individual possessing a valid permit issued by the director of health pursuant to R.C. 3701.143 of the Revised Code.”)
\textsuperscript{104} \textsc{Donald J. Ramsell, Understanding DUI Scientific Evidence: Leading Defense Attorneys on Understanding Chemical and Chemical and Field Sobriety Testing Procedures, Analyzing the Validity of Results, and Developing Trial Strategies, Standards in DUI/DWI Cases} (2d ed. 2009) (“Essentially, most states have statutes that grant their departments of public health or departments of state police authority to establish methods of testing in DUI and DWI cases that replace the traditional predicates [\textit{Daubert} or \textit{Frye} standards] for the admission of scientific tests. Where such standards do exist, the burden then shifts to the opponent of the evidence to establish the invalidity of the scientific testing or methods involved.”).
\textsuperscript{105} \textit{Id.}
accuracy and reliability of database results and found in favor of the defendant’s right to confrontation. With general information databases, the courts seem ready to allow defense access to the database information in order to challenge admissibility of the database results.107 The more technologically scientific the database, however, the more courts seem reluctant to permit challenges to the admissibility of results and instead default to either the legislature or another court’s determination of the accuracy and reliability of the database and the technology involved.108 Yet even with the arguably most accurate and reliable databases and technology, mistakes happen, forcing the courts and legislatures to see the exculpatory value in allowing the accused to challenge the database information and technology against him.109

Courts have upheld the defendant’s right to confrontation with general information databases. For example, in United States v. Dioguardi, state witnesses collected certain data of inventory, purchases, and sales for evidence of bankruptcy violations.110 The information was put into a database and ran through a program.111 The state produced the computer printouts, which indicated fraudulent transferring and concealing property of a bankruptcy, but the state refused to produce the specific program in discovery.112 Without this specific information, the defense argued they could not effectively cross-examine the printouts.113 The Second Circuit held that the defense was entitled to all of the information:

It is quite incomprehensible that the prosecution should tender a witness to state the results of a computer’s operations without having the program available for defense scrutiny and use on cross-examination if desired. We place the Government on the clearest possible notice of its obligation to do this and also of the great desirability of making the program and other materials needed for cross-examination of computer witnesses, such as flow-charts used in the preparation of programs, available to the defense a reasonable time before trial.114

108. See e.g., infra text accompanying notes 116-119.
109. See generally Kimberly Cogdell Boies, Misuse of DNA Evidence is Not Always a “Harmless Error”: DNA Evidence, Prosecutorial Misconduct, and Wrongful Conviction, 17 TEX. WESLEYAN L. REV. 403 (2011). “Issues related to collection interpretation and application are applicable to DNA evidence.” Id. at 407. “Other common problems regarding the admissibility and reliability of DNA evidence include: lab proficiency, contamination, lack of written protocols, accreditation, technique, quality control, chain of custody and temperature regulation.” Id
111. Id.
112. Id. at 1038.
113. Id.
114. Id.
The court realized that even with simple technology, the defense is entitled to cross examine the way a program works and the accuracy of the results that are produced.

Similarly, in *New Jersey v. Fortin*, the state called an expert to testify to unique similarities between the victim and a woman sexually assaulted by the defendant. The state refused to give the defense information that was used to form the expert’s conclusions. The New Jersey Supreme Court found that the defense must have an adequate opportunity for cross-examination of database results. The court noted that without having access to a database of violent sexual assault cases that the expert had investigated, studied, or analyzed, and the modus operandi and characteristics of those crimes, the defense had no way to verify whether the expert’s conclusions were valid.

Even though DNA is thought to be “the most reliable form of identification in modern society,” courts have also recognized the defendant’s right to confront DNA database output. While the courts have not necessarily been willing to give the defense unfettered access to the database, they have given defendant’s limited access or upheld subpoenas for certain facts regarding the database and the actual search results, as opposed to an expert’s opinion based on those results.

While these examples deal with a wide range of databases and information, they are similar to the breath test defendant’s request for COBRA data in that COBRA data is information contained in a state database that may include exculpatory information and allow the defense to show reasonable doubt as to the accuracy and reliability of database output, or a breath test result.

From a different, yet still broader perspective, the issue is one of advancement in technology. In *Melendez-Diaz*, the Supreme Court held that the defense must have the opportunity to cross examine the analyst if forensic test results are to be admitted. The Court noted past serious deficiencies in forensic analysis methods and erroneous convictions based on discredited forensics. The Court noted a study in which 60% of wrongful criminal

---

116. Id.
117. Id. at 1000-01.
118. Id. at 1002.
120. Strutin, *supra* note 13, at 49-54.
123. Melendez-Diaz v. Massachusetts, 557 U.S. 305 (2009). At issue was a certificate from the forensic laboratory certifying that the tested substance was cocaine. Id.
124. Id. at 319 (citing Pamela R. Metzger, *Cheating the Constitution*, 59 VAND. L. REV. 475, 491 (2006)).
convictions were related to invalid forensic testimony.125 “A vigorous cross-examination of programmers can shed light on the assumptions on which technicians rely and reveal the strengths and weaknesses of the methods used.”126

The same rational applies to COBRA data. While the database is not a type of forensic analysis, it is a new advancement in technology, the data subject to human error or manipulation at every step. “‘[T]here is wide variability across forensic science disciplines with regard to techniques, methodologies, reliability, types and numbers of potential errors, research, general acceptability, and published material.’”127 A judge acting as gatekeeper in determining the minimum requirements for admissibility of technical evidence should not inherently foreclose the defendant from full confrontation and cross-examination of the accuracy and reliability of the technology used against him.

Another closely related issue in technology that has been at the forefront of litigation is that of breath testing machine source codes. Source codes are created by computer programmers and the codes contain “the commands for sequencing the operation of the machine, data entry questions, operational parameters and mathematical formulas necessary for breath testing.”128 The source code is similar to COBRA data in that the machine source code goes directly to the accuracy and reliability of a breathalyzer.129 The breath test operator simply responds to the prompts of the machine that occur due to the programming of the source code. Thus, the defense is unable to adequately cross examine how the machine works when confronting the operator rather than the programmer.130 Yet even with source codes, numerous courts have required production, noting the defendant’s right to confrontation and the importance of breath test results in DUI prosecutions.131

IV. CONCLUSION

“In courts of law, forensic testimony often goes unchallenged by a scientifically naive legal community. Forensic methods must be screened with

125. Melendez-Diaz, 557 U.S. at 319 (citing Brandon L. Garret & Peter J. Neufeld, Invalid Forensic Science Testimony and Wrongful Convictions, 95 CA. L. REV. 1, 14 (2009)); see also James M. Shellow, The End of a Confidence Game: A Possible Defense to the Impossible Drug Prosecution, The Champion 22, 24 (2000) (referencing color testing methods used to identify drugs were later found to have revealed false positives 20 – 30% of the time, and crystal tests used to identify drugs, which also turned out to be an unreliable method of drug testing).
128. Palmer, supra note 2, at 415 (citing Fargo v. Levine, 747 N.W.2d 130, 132 (N.D. 2008)).
129. Workman, Jr., supra note 73, at 2.
130. See generally Palmer, supra note 2.
131. See generally 1 HANDLING DRUNK DRIVING CASES §16:27 (2d ed. 2014)
greater care if [equal] justice is to be served.”

Under the per se statutory scheme, a breath test result alone can convict. “In few other situations is a single piece of evidence so vital to a case’s success or failure.” The criteria for removal of a [breath testing] machine from service is a 52% failure in a 55 test window. This means a machine is considered to be working properly even though it cannot produce a valid result more than half of the times it is used.

Without access to the full spectrum of COBRA data available, “Defendants are left with no option but to accept that the machine performed properly in their case and the results are accurate whether that is the truth or not.” To ensure a DUI breath test defendant’s rights to confrontation and a fair trial, COBRA data must be discoverable.


134. Workman, Jr., *supra* note 9, at 217.
