ADMINISTRATION

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

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

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

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

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

JENNIFER A. KREDER, B.A., J.D.
Associate Dean for Law School Affairs & Professor of Law

HEATHER CRABBE, B.S., J.D.
Assistant Dean of Students

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

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

JENNIFER KINSLY, B.A., J.D.
Director of Experiential Learning & Professor of Law

KERRY KLUMPE, B.A., J.D.
Director of Communications

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

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

DAVID SINGLETON, B.A., J.D.
Director of Constitutional Litigation Clinic & Professor of Law

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

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

FACULTY

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

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

ANTHONY E. CHAVEZ, B.S., J.D.
Professor of Law

URSULA DOYLE, B.A., M.A., J.D.
Associate Professor of Law

CAROL FURNISH, B.A., M.L.S.
Professor of Library Services

CHRISTOPHER GULINELLO, B.A., J.D., LL.M.
Professor of Law

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

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

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

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

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 KINSLY, B.A., J.D.
Professor of Law & Director of Experiential Learning

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

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

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

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

LAWRENCE ROSENTHAL, B.A., J.D., LL.M.
Associate Dean for Academics & 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
JEFFREY STANBLEN, A.B., J.D.
Dean & 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
BARBARA WAGNER, B.A., M.S.B.A., J.D.
Assistant Professor of Law & Director of Small Business & Nonprofit Law Clinic
MICHAEL WHITEMAN, B.A., M.S.L.S., J.D.
Associate Dean for Library Services and Information Technology & Professor of Law

EMERITI FACULTY
WILLIAM R. JONES, B.S., M.A., J.D.

ADJUNCT FACULTY
MARK ARNZEN B.S., B.A., J.D.
DONYETTA BAILEY, B.S., J.D.
DAVID BARRON, J.D.
HON. GREGORY M. BARTLETT, A.B., M.A., J.D.
JOHN BENINTENDI, J.D.
HELEN GULGUN BULKULMEZ, B.A., J.D.
MIKE CARR, 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.
DAVID DORTON, B.A., J.D.
ROBERT FURNIER, B.A., J.D.
AMANDA GERKEN, 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, B.A., J.D.
PENNY HENDY, B.A., J.D.
DAN HUNT, B.A., J.D.
DAVID JEFFERIES, B.A., J.D.
RICHARD KATZ, B.A., J.D.
PENNY LANDEN, B.A., J.D.
MATTHEW LAWLESS, B.A., J.D.
J.B. LIND, B.A., J.D.
WILLIAM LUNS福德, B.A., J.D.
HON. ROBERT LYNNS, B.A., J.D.
JACOB D. MAHLE, B.A., J.D.

KATE MOLLOY, B.A., J.D.
JOSEPH MORDINO, J.D.
FRANK MUNGO, B.S., J.D.
DANIEL MURNER, B.A., J.D.
COL. OWENS, B.A., J.D.
SEAN OWENS, B.A., J.D.
MARC PERA, 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.
ADAM C. SHERMAN, B.A., J.D.
GREGORY SIZEMORE, B.A., J.D.
NATHANIEL SIZEMORE, B.A., J.D.
CHRISTEN STEIMLE, B.A., J.D.
HON. DOUGLAS STEPHENS, B.A., J.D.
Tiffany Stevens, B.A., J.D.
JOSEPH TANSINO, 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.
SCOTT VAN NICE, B.A., J.D.
AL WEISBROD, J.D.
ELIZABETH WINECHELL, J.D.
J. STEPHEN WIRTHLIN, JR., B.A., J.D.
ELIZABETH ZINK-PEARSON, J.D.
ARTICLES

Information Security, Confidentiality, and Cyber Ethics for Law Entities
Thomas Doty, Esq., LL.M. ...................................................................................................................... 1

The United States’ Perspective on Data Protection in Financial Technology (Fintech), Insurance, and Medical Services
Joseph Dehner .......................................................................................................................................... 13

Trends for Potential Insurance Coverage for Losses Arising From a Data Breach
Nathan L. Colvin and Timothy C. Dougherty .......................................................................................... 29

Merchant Liability to Financial Institutions for a Data Breach
J.B. Lind, et al. ........................................................................................................................................... 35

Government Enforcement When Private Date Information is Breached: Guidance and Best Practices
Jacob D. Mahle, Nathan L. Colvin, and Emily St. Cyr ........................................................................... 41

Consumer Class Actions Arising From Data Breaches Present a Battleground for Standing to Bring Suit
Eric W. Richardson, Nathan L. Colvin, and Timothy C. Dougherty ....................................................... 49

NOTES

A “Golden Key” to Pandora’s Box: The Security Risks of Government-Mandated Backdoors to Encrypted Communications
Alexa Wainscott ...................................................................................................................................... 57

The Computer Fraud and Abuse Act: Punishing Hackers and Solving Employment Disputes in the Same Statute
Rob Spicer ................................................................................................................................................. 83
SPECIAL THANKS TO JEANNINE ABUKHATER LAMBERT, ESQ., WITHOUT WHOM THE SYMPOSIUM ACCOMPANYING THIS ISSUE WOULD NOT HAVE BEEN POSSIBLE.
INFORMATION SECURITY, CONFIDENTIALITY, AND CYBER ETHICS FOR LAW ENTITIES*

Thomas Doty, Esq, LLM**

I. INTRODUCTION

“The law does not speak well to technical issues.” Joe Dehner boldly delivered this nugget of clarity to a packed room during the “Global Privacy and the Clash Between Privacy, Convenience and Security” session at the 9th Annual NKU Cybersecurity Symposium. 1

Mr. Dehner’s words took me back almost 20 years when the executive powers that be “informed” me that my career as a DARPA-trained engineer was being transitioned to a law position. My technical expertise as the Technology Manager supporting the High Performance Computing group were needed in the law field because “it was easier to teach law to a geek, than geek to a lawyer.”

Law school was a difficult transition for the left brain linear problem solver who now needed to be a right brain student of the law. I was an engineer in a room full of academics, who had spent their entire scholastic life honing their skill sets of argument and written communications, constantly reminding the law professor that they entered this course of study because they hated math and science. Twenty years later, the circular reasoning of technology competency has evolved from the 1990s “Unfrozen Caveman Lawyer”2 skits to demand that 21st century lawyers must be competent in technology or affiliate with a “geek” who is.

The competitive advantage of a left brain versus right brain skill set, especially when it relates to the 21st century practice of law, has only accelerated as the left side understanding of technology has become a critical weapon in the arsenal of the modern day law practitioner. The left brain concept is further supported by the fact that most humans are left brain dominant3 and that lawyers,

---

* Copyright © 2016 NKU; Thomas Doty
** Thomas Doty is the Director of Intellectual Asset Protection at NuStrategies, LLC, a collaboration of “reformed attorneys” and new model technology strategists. He obtained his LLM in Intellectual Property from the University of New Hampshire (formerly Franklin Pierce Law Center) in 2002 with a focus on business and technology.
2. Saturday Night Live (NBC television broadcast 1991-96) (“The Unfrozen Caveman Lawyer” was a recurring character created by Jack Handey and played by Phil Hartman on Saturday Night Live.).
3. Peter F. MacNeilage et al., Evolutionary Origins of Your Right and Left Brain, SCIENTIFIC AMERICAN, July 1, 2009, at 60.
judges and bankers tend to be left-brained. These factors lay the foundation that all legal practitioners have an ethical and legal duty to be technically competent.

II. COMPETENT REPRESENTATION REQUIRES TECHNICAL COMPETENCE

Since the American Bar Association (“ABA”) House of Delegates adopted the ABA Model Rules of Professional Conduct (“Rules”) in 1983, there has been an ethical obligation related to competent representation. The ABA recently clarified that legal counsel must also stay current on technological risks and take reasonable action to protect against those risks. The increase of data breaches involving law entities prompted the ABA to demand that counsel elevate their cybersecurity awareness of the process associated with the data they retain in support of client representation. The ABA reasoned that the disclosure of client’s information addressed under Rule 1.6 would immediately invoke Rule 1.4. Under the Rules, the attorney-client privilege will protect confidential communications between the attorney and client in cases of inadvertent disclosure only if the attorney and client act reasonably to protect that privilege. The State Bar of California opined that a lack of reasonable care to protect against disclosing privileged and protected information when handling any Electronically Stored Information (ESI) can be deemed a waiver of the attorney-client privilege. What “reasonable care” means, however—especially in a

5. MODEL RULES OF PROF’L CONDUCT (AM. BAR ASS’N 1983) [hereinafter “MODEL RULES”].
6. MODEL RULES r. 1.1 (AM. BAR ASS’N 1983) (discussing the attorney’s duty of competence).
7. MODEL RULES r. 1.1, cmt. 8 (AM. BAR ASS’N 1983) (clarifying that “[t]o maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject.”).
8. MODEL RULES r. 1.6, cmt. 18 (AM. BAR ASS’N 1983) (discussing the lawyer’s duty to keep information confidential, stating “[p]aragraph (c) [to Rule 1.6] requires a lawyer to act competently to safeguard information relating to the representation of a client against unauthorized access by third parties and against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are subject to the lawyer’s supervision.”). Comment 19 clarifies that the lawyer “must take reasonable precautions to prevent the information from coming into the hands of unintended recipients.”).
10. See MODEL RULES r. 1.6 (AM. BAR ASS’N 1983) (providing under Rule 1.6(c), “[a] lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client.”).  
context involving complex technological issues with potential risk—is not always clear-cut.12 “Reasonable” or “Reasonably,” when used in relation to a lawyer’s conduct, “denotes the conduct of a reasonably prudent and competent lawyer.”13 The application of the reasonable standard has been challenged due to the conflicts with the requirements under Rule 1.15, Comment 1, which states that “[a] lawyer should hold property of others with the care required of a professional fiduciary.”14 According to the Law Dictionary, a “fiduciary is a person holding the character of a trustee, or a character analogous to that of a trustee, in respect to the trust and confidence involved in it and the scrupulous good faith and candor which it requires.”15 This fiduciary standard under Rule 1.15(a) includes the client’s digital assets and intellectual property, held by the attorney locally or in the cloud, to assure that that property is ethically and technically safeguarded.16 Additionally, under Rule 1.16(d), the lawyer must manage the handling of all documents including storage, return and protection of all electronically stored information.17

procedures employed were unreasonable); see also FED. R. OF EVID. 502(b) (“Inadvertent Disclosure. When made in a federal proceeding or to a federal office or agency, the disclosure does not operate as a waiver in a federal or state proceeding if: (1) the disclosure is inadvertent; (2) the holder of the privilege or protection took reasonable steps to prevent disclosure; and (3) the holder promptly took reasonable steps to rectify the error, including (if applicable) following Federal Rule of Civil Procedure, rule 26 (b)(5)(B).”)

12. See MODEL RULES r. 1.6, cmt. 18 (“Acting Competently to Preserve Confidentiality . . . The unauthorized access to, or the inadvertent or unauthorized disclosure of, information relating to the representation of a client does not constitute a violation of paragraph (c) if the lawyer has made reasonable efforts to prevent the access or disclosure. Factors to be considered in determining the reasonableness of the lawyer’s efforts include, but are not limited to, the sensitivity of the information, the likelihood of disclosure if additional safeguards are not employed, the cost of employing additional safeguards, the difficulty of implementing the safeguards, and the extent to which the safeguards adversely affect the lawyer’s ability to represent clients (e.g., by making a device or important piece of software excessively difficult to use).”), http://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_1_6_confidentiality_of_information/comment_on_rule_1_6.html.

13. MODEL RULES r. 1.0(h) (AM. BAR ASS’N 1983).


15. THE LAW DICTIONARY, THELAWDICTIONARY.ORG (defining a fiduciary as a person “who is invested with rights and powers to be exercised for the benefit of another person”), http://thelawdictionary.org/fiduciary/ (last visited Feb. 2, 2017); see also Cornell Univ. Law Sch., Fiduciary Duty (noting that the fiduciary duty is the “highest standard of care”), https://www.law.cornell.edu/wex/fiduciary_duty (last visited Feb. 2, 2017); see also Svanoe v. Jurgens, 33 N.E. 955, 956-57 (Ill. 1893) (defining the role of a fiduciary).

16. See MODEL RULES R. 1.15(a) (AM. BAR ASS’N 1983)(discussing “other property,” aside from funds, that “shall be identified . . . and appropriately safeguarded”).

17. See MODEL RULES r. 1.16(d) (AM. BAR ASS’N 1983)(providing that upon termination of representation, a lawyer “shall take steps to the extent reasonably practicable to protect a client’s interests, such as . . . surrendering papers and property to which the client is entitled”); see also MODEL RULES R. 1.16, cmt. 9 (adding that even if the termination was unfair, “a lawyer must take all reasonable steps to mitigate the consequences to the client”).
As the technology and associated processes used in the practice of law has advanced, the level of technological competence of legal counsel has lagged behind. According to the 2016 ABA statistics, 62% of practicing attorneys age 45 or older did not grow up with computers and similar modern technology.\(^{18}\) This deficiency is multiplied by the newest generation to enter the profession, who have only embraced technology through social media or applications like Westlaw Next or Lexis Advance.

### III. Issues of Millennial Technical Competence

Although American millennials (Gen Y, ages 16 - 34) are hyper-connected, they are nevertheless under-skilled and lack tech savvy.\(^{19}\) Millennials spend an average of 35 hours per week on digital media,\(^{20}\) but 58% of PIACC\(^{21}\) test takers are unable to complete basic computer tasks.\(^{22}\) American millennials ranked last out of 19 countries that tested technical competency skills.\(^{23}\) A 2015 UCLA Freshman Survey disclosed that 94.8% of the freshmen were using online networks like Facebook, but only 38.1% of incoming college freshmen self-identified themselves as above average in computer skills, compared to people their age.\(^{24}\) This same survey also disclosed that 3.2% of students identified a computer-related planned field of study.\(^{25}\)

Gen Y Americans lag far behind their overseas peers in every measure, but they even score lower than other age groups of Americans, scoring in a four-way

---


21. *What is PIACC?*, Nat’l Ctr. for Educ. Statistics (explaining that PIACC is The Program for the International Assessment of Adult Competencies, which is a cyclical, large-scale study developed under the Organization for Economic Cooperation and Development (“OECD”). PIACC’s goal is to assess and compare the basic skills and competencies of adults around the world.), https://nces.ed.gov/surveys/piaac/ (last visited Feb. 3, 2017).

22. *See OECD, CHANGE THE EQUATION* (explaining a basic task to be using one function within a generic interface or sorting, searching for, and emailing information from a spreadsheet), http://www.changentheequation.org/ (last visited Oct. 30, 2016).


25. *Id.*
tie for last place with the Slovak Republic, Ireland, and Poland.\textsuperscript{26} One professor at the University of Notre Dame reported that many of his students didn’t even know how to navigate menus in productivity applications when related to the smart use of technology.\textsuperscript{27}

Amani Smathers, an attorney in Michigan, described 20th century lawyers as “I-shaped,” having deep legal knowledge and skills, but declared that 21st century lawyers must be “T-shaped.”\textsuperscript{28} A T-shaped lawyer still has deep legal expertise but also has the ability to collaborate across many disciplines, such as technology, business, analytics, and data security.\textsuperscript{29} The changes in the legal market, lawyer ethics and new positions for lawyers reinforce the Model Rules comments that lawyers must be reasonably informed about relevant technology including local technology (technology controlled by lawyers and their employees), cloud computing (technology controlled by third parties and accessed over the Internet), and traditional and cloud based software (SaaS). Clients are demanding higher technological competency from their lawyers and law firms including vendor assessment standards similar to those of D. Casey Flaherty, corporate counsel at Kia Motors America, who created and implemented a technology audit for the firms that worked with Kia.\textsuperscript{30} Flaherty found that the lawyers lacked basic technology competence, and the resulting inefficiencies led to unnecessary costs for his company.\textsuperscript{31} He made firms slash their fees until they could pass the assessment.\textsuperscript{32}

IV. AS TRUSTED ADVISORS, LAWYERS MUST SECURE THEIR INFORMATION

Basic knowledge of cybersecurity has become an essential lawyer competency.\textsuperscript{33} Beginning in 2009, state and federal law enforcement agencies warned larger United States law firms that their computer files were targets for cyber spies and thieves.\textsuperscript{34} These cyber spies and thieves look for valuable

\begin{footnotes}
\item[26.] Anne Fisher, \textit{American Millennials are among the world’s least skilled}, FORTUNE.COM (Mar. 10, 2015), http://fortune.com/2015/03/10/amERICAN-millennials-are-among-the-world' S-leAST-skilled/.
\item[27.] Proffitt, \textit{supra} note 29.
\item[29.] Id.
\item[30.] Id.
\item[31.] Id.
\item[32.] Id.
\item[33.] See ABA Commission on Ethics 20/20, AMERICANBAR.ORG, http://www.amERICANbar.org/groups/professional_responsibility/aba_commission_on_ethics_20_20.html (last visited Feb. 2, 2017), (explaining that the Commission was created in 2009 to study how the Model Rules of Professional Conduct should be updated in light of globalization and changes in technology)
\item[34.] See Lolita C. Baldor, \textit{FBI: Hackers targeting law and PR firms}, NBCNEWS.COM (Nov. 17, 2009, 10:58 AM ET), (discussing how the FBI warned of “noticeable increases” in efforts to hack into the computer systems of law firms and public relations companies).
\end{footnotes}
information about potential corporate mergers, patent and trademark secrets, litigation plans, and financial data of corporate clients.\(^{35}\)

In 2010, the State Bar of California considered whether attorneys violated the duty of confidentiality when the attorneys transmitted and stored confidential information with technology that was susceptible to unauthorized access.\(^{36}\) The California Bar analyzed this issue in the context of the attorney’s duty of competence, concluding:

An attorney’s duties of confidentiality and competence require the attorney to take appropriate steps to ensure that his or her use of technology in conjunction with a client’s representation does not subject confidential client information to an undue risk of unauthorized disclosure. Because of the evolving nature of technology and differences in security features that are available, the attorney must ensure the steps are sufficient for each form of technology being used and must continue to monitor the efficacy of such steps.\(^{37}\)

This cybersecurity demand to bar organizations resulted in ABA Resolution 109, which calls for firms to “develop, implement, and maintain an appropriate cybersecurity program.”\(^{38}\)

Lawyers will never be able to guard against every cybersecurity threat. However, failing to take reasonable precautions threatens the confidentiality of clients’ information and puts them at a greater risk of discipline, malpractice claims, reputational and client loss.

V. DUTY OF COMPETENCE – RULE 1.1

As a multi-jurisdictional attorney who practices in California, this ethical duty to be technically competent was formally introduced by CA Formal Ethics No. 2010-179, which provides:

---

35. Id.
36. See generally Cal. State Bar Standing Comm. On Prof’l Resp. and Conduct, Formal Op. 2010-179 (2010) [hereinafter “Formal Op.”], http://ethics.calbar.ca.gov/LinkClick.aspx?fileticket=wmqECiHp7h4%3D&tabid=836 (Specifically, the California Bar reviewed a matter in which an attorney used his personal laptop to work on a client’s information from home; access a public Wi-Fi network to conduct legal research for the client’s matter; and communicate via email with the client while away from his office.).
37. Id.
38. Cybersecurity Legal Task Force Section of Science & Tech. Law, AM. BAR ASS’N, Report to the House of Delegates 14 (Aug. 2014), http://www.americanbar.org/content/dam/aba/events/law_national_security/2014annualmeeting/ABA%20-%20Cyber%20Resolution%20109%20Final.authcheckdam.pdf (last visited Oct. 30, 2016) (addressing cybersecurity issues that are critical to the national and economic security of the United States. The Report encourages private and public sector organizations to develop, implement, and maintain an appropriate cybersecurity program that complies with applicable ethical and legal obligations and is tailored to the nature and scope of the organization and the data and systems to be protected.).
An attorney’s duties of confidentiality and competence require the attorney to take appropriate steps to ensure that his or her use of technology in conjunction with a client’s representation does not subject confidential client information to an undue risk of unauthorized disclosure. Due to the evolving nature of technology and disparity in security features that are available, the attorney must ensure the process undertaken is sufficient for each form of technology being used and must continue to monitor the efficacy of such steps.39

Rule 1.1 specifically states that “[a] lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation.”40 Comment 8 to Rule 1.1 provides authoritative guidance, stating “[t]o maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject.”41

Formally embracing the ABA focus on the critical role technology has taken in the practice of law, 26 states have adopted Comment 8 of the Model Rules 1.1 either by statute or formal opinion.42 Positioning Florida lawyers with an advantage in cultivating business, on September 29, 2016, the Florida Supreme Court approved a rule mandating for the first time in 31 years that state lawyers take a minimum of three hours technology-related CLE courses, taking effect Jan. 1, 2017.43

A. Duties of Communication, Confidentiality, Safekeeping Property – Rules 1.4, 1.6, 1.15 and 1.16

As a critical skill to 21st century legal representation, I propose technical competence is the cornerstone to interpreting and executing compliance of the Rules. Similar to the California Ethics No. 2010-179, New York identified the

40. MODEL RULES r. 1.1(AM. BAR ASS’N 1983).
41. See MODEL RULES r. 1.1 cmt. 8(AM. BAR ASS’N 1983)..
43. See In re Amendments to Rules Regulating the Florida Bar 4–1.1 and 6–10.3, 200 So.3d 1225 (Mem), 1226–28 (Fla. 1992); see also Mark D. Killian, Court approves CLE tech component, THE FLORIDA BAR NEWS, https://www.floridabar.org/DIVCOM/JN/jnnews01.nsf/8e9f13012b96736985256aa900624829/3b05732accd9edd28525803e006148cflOpenDocument (last visited Oct. 30, 2016).
strategic advantage for its members in 2010 with NY Ethics Opinion 842, which endorsed and expanded the technical requirement to state that “(a) Lawyer should stay abreast of technological advances to ensure that the storage system remains sufficiently advanced to protect the client’s information, and should monitor the changing law of privilege to ensure that storing the information online will not cause loss or waiver of any privilege” Rules: 1.4, 1.6(a), 1.6(c).44

Rule 1.4 – Communication, defines the what, why, when and how we communicate with clients stating that “(a) A lawyer shall: (1) promptly inform the client of any decision or circumstance with respect to which the client’s informed consent, as defined in Rule 1.0(e), is required by these Rules.”45 The mishandling of a client’s information would be defined by the Comment on Rule 1.4 [2] when “a particular decision about the representation be made by the client, paragraph (a)(1) requires that the lawyer promptly consult with and secure the client’s consent prior to taking action unless prior discussions with the client have resolved what action the client wants the lawyer to take.”46 The “how” component is specifically addressed under Rule 1.0 (e) defining “Informed consent.” This denotes the agreement by a person to a proposed course of conduct after the lawyer has communicated adequate information and explanation about the material risks of and reasonably available alternatives to the proposed course of conduct.47 Whether a lawyer may “be required to take additional steps in order to comply with other law, such as state and federal laws that govern data privacy or that impose notification requirements upon the loss of, or unauthorized access to, electronic information” is further clarified under Comment on Rule 1.6 [18].48

Rule 1.6 - Confidentiality of Information identifies the entry point to future cyber claim issues of the legal provider and states “(a) A lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent, the disclosure is impliedly authorized in order to carry out the representation…”,49 highlighting a fundamental principle in the client-lawyer relationship that, in the absence of the client’s informed consent, the lawyer must not reveal information relating to the representation. This rule prohibiting a lawyer from revealing information relating to the representation of a client also applies to disclosures by lawyers that do not in themselves reveal protected information but could reasonably lead to the discovery of such information by a third person.50 The principle of client-lawyer confidentiality is given effect by related bodies of law such as the attorney-client privilege, the work product

45. See MODEL RULES r. 1.4 (AM. BAR ASS’N 1983).
46. See MODEL RULES r. 1.4 cmt. 2 (AM. BAR ASS’N 1983).
47. See MODEL RULES r. 1.0(e) (AM. BAR ASS’N 1983).
48. See MODEL RULES r. 1.6 cmt. 18 (AM. BAR ASS’N 1983).
49. Id. at r. 1.6(a).
50. MODEL RULES r. 1.6 cmt. 4 (AM. BAR ASS’N 1983).
doctrine and the rule of confidentiality established in professional ethics.\textsuperscript{51} The confidentiality rule applies not only to matters communicated in confidence by the client, but also to all information relating to the representation, whatever its source.\textsuperscript{52}

The escape clause from an engineering course is communicated in Rule 1.6, Comment 9, clarifying that “a lawyer’s confidentiality obligations do not preclude a lawyer from securing confidential legal advice about the lawyer’s personal responsibility to comply with these Rules.” In most situations, disclosing information to secure such advice will be impliedly authorized for the lawyer to carry out the representation.\textsuperscript{53} This comment could also be expanded to affiliating with competent technical service providers that have been properly investigated and vetted.

Further expansion of professional technical affiliation is also interpreted under Rule 1.6 Comment [18]:

\textbf{[18]} \textit{Paragraph (c) requires a lawyer to act competently to safeguard information relating to the representation of a client against unauthorized access by third parties and against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are subject to the lawyer’s supervision…The unauthorized access to, or the inadvertent or unauthorized disclosure of, information relating to the representation of a client does not constitute a violation of paragraph (c) if the lawyer has made reasonable efforts to prevent the access or disclosure.}\textsuperscript{54}

Comment 18 provides guidance regarding implementing measures in protecting the unauthorized access to, or the inadvertent or unauthorized disclosure of, information relating to the representation of a client that does not constitute a violation of paragraph (c) if the lawyer has made reasonable efforts to prevent the access or disclosure. Factors to be considered in determining the reasonableness of the lawyer’s efforts include, but are not limited to, the sensitivity of the information, the likelihood of disclosure if additional safeguards are not employed, the cost of employing additional safeguards, the difficulty of implementing the safeguards, and the extent to which the safeguards adversely affect the lawyer’s ability to represent clients (e.g., by making a device or important piece of software excessively difficult to use).\textsuperscript{55}

\begin{itemize}
\item \textsuperscript{51} \emph{See id.} at cmt. 3.
\item \textsuperscript{52} \emph{Id.}
\item \textsuperscript{53} \emph{See id.} at cmt. 9.
\item \textsuperscript{54} \emph{See id.} at cmt. 18.
\item \textsuperscript{55} \emph{Id.}
\end{itemize}
This is reminiscent of the “calculus of negligence”, a classic example of a balancing test, first defined by Judge Learned Hand in United States v. Carroll Towing Co.\textsuperscript{56}

Comment 18 further places a potential heightened level of information protection by stating, “a client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to forgo security measures that would otherwise be required by this Rule.”\textsuperscript{57}

The duty of confidentiality and the competent handling of client information is also applied to past, present and future clients under Rule 1.15 Safekeeping Property\textsuperscript{58}, Rule 1.16 Declining or Terminating Representation\textsuperscript{59} and Rule 1.18 Duties to Prospective Client.\textsuperscript{60}

**B. Technical Affiliation and the Duty to Supervise - Rules 5.1 and 5.3**

The reasonable efforts required to prevent unauthorized access demand, at the very least, that attorneys have diverse technological knowledge about protecting client data, and be able to either implement the required processes and technology or find experts who can.\textsuperscript{61} Rule 5.1 provides guidance on the duty to supervise as it relates to a partner or supervisory lawyer.\textsuperscript{62} Rule 5.1(c)(2) represents that attorneys supervising other lawyers must take reasonable steps to become knowledgeable about the actions of those attorneys in representing clients of the firm, which would include the handling of all ESI; understanding the technological experience of co-counsel and their consultants/experts; confirming that confidentiality protections are being maintained and client data is being stored and transmitted securely; and staying well-informed of data handling during the discovery process and supervising decisions.\textsuperscript{63}

Model Rule 5.3 and Comment [3] provide that a lawyer may use nonlawyers outside the firm or General Counsel office to assist the lawyer in rendering legal

\textsuperscript{56} See United States v. Carroll Towing Co., 159 F.2d 169 (2d. Cir. 1947).
\textsuperscript{57} Model Rules r. 1.6 cmt. 18 (AM. BAR ASS’N 1983).
\textsuperscript{58} See Model Rules r. 1.15 cmt. (AM. BAR ASS’N 1983).
\textsuperscript{59} See id.
\textsuperscript{60} Model Rules r. 1.18(b) (AM. BAR ASS’N 1983); see also Model Rules r. 1.18 cmt. 9 (AM. BAR ASS’N 1983).
\textsuperscript{61} See David G. Reis, Cyber Security for Attorneys: Understanding the Ethical Obligations, Law Practice Today 2 (Mar. 2012), http://www.americanbar.org/content/dam/aba/publications/law_practice_today/cyber-security-forattorneys-understanding-the-ethical-obligations.authcheckdam.pdf. (“[Model Rule 1.1] requires attorneys who lack the necessary technical competence for security (many, if not most attorneys) to consult with qualified people who have the requisite expertise.”); see also JILL D. RHODES & VINCENT I POLLEY, THE ABA CYBERSECURITY HANDBOOK: A RESOURCE FOR ATTORNEYS, LAW FIRMS, AND BUSINESS PROFESSIONALS 66 (2013) [hereinafter ABA CYBERSECURITY HANDBOOK] (“Getting expert help is a recurring theme (as well as good advice) in ethics opinions on this subject.”); see also CAL. R. PROF. CONDUCT 3-110(C) (associating with other attorneys or learning needed skills to satisfy competence requirement).
\textsuperscript{62} Model Rules r. 5.1 (AM. BAR. ASS’N 1983).
\textsuperscript{63} See id. at r. 5.1(c)(2); see also id. at cmt. 2, 3, and 5.
services to the client. Comment [4] expands allowable outside assistance to nonlawyer service providers, when sharing information with nonlawyers outside the lawyer’s own firm and ensuring others protect and maintain client confidentiality. These rules require supervision of a provider of online storage and data security practices, just as they require supervision of an offsite provider of services such as a hard copy record storage warehouse. While attorneys can meet their duty of competence by bringing in an outside expert, the duties of confidentiality and competence are ongoing and not delegable.

VI. SUMMARY AND CONCLUSION

With compromised data records totaling over 554,454,942 for the first half of 2016, Vincent I. Polley, lawyer and co-author of The ABA Cybersecurity Handbook, has stated “a lot of firms have been hacked, and like most entities that are hacked, they don’t know that for some period of time. Sometimes, it may not be discovered for a minute or months and even years.” When a firm is breached, all of the firm’s data can be revealed, expanding the scope for litigation considerably, including actions for client’s data being compromised while in the firm’s possession. According to Aviva, after your company is breached, 60% of your customers will think about moving and 30% actually do. One-third of consumers said they would stop dealing with a business following a cybersecurity breach, even if they do not suffer a material loss. “Attorneys first and most important job is to represent their client zealously. If firms do not pay attention to the unique challenges that technology presents and do not actively protect against those challenges, they can end up losing clients and costing

64. See MODEL RULES OF PROF’L CONDUCT r. 5.3 (AM. BAR ASS’N 1983); see also id. cmt. 2, 3, and 5.
67. See Rhodes & Polley, supra note 66.
themselves money,” Richard Susskind embraced those challenges and expressed that the changes in the legal profession would mean a different role for lawyers in the future when he theorized that “it is simply inconceivable that information technology will radically alter all corners of our economy and society and yet somehow legal work will be exempt from any change.”

Counter to the thought that any lawyer can comprehend and apply the complexities of rapidly changing technology, access to justice for clients can only be assured by technically competent lawyers. Therefore, you should think like a geek, perform like a lawyer.

71. Jordan McQuown, Chief Information Officer at LogicForce Consulting.
THE UNITED STATES’ PERSPECTIVE ON DATA PROTECTION IN FINANCIAL TECHNOLOGY (FINTECH), INSURANCE, AND MEDICAL SERVICES

Joseph Dehner*

I. INTRODUCTION

With the increasing prevalence and importance of the collection, use, analysis and manipulation of big data, and the potential privacy concerns that it can raise, big data has touched consumers, industry groups, and policy makers alike in the United States. In contrast to its European counterparts, the United States does not regulate big data through a single comprehensive data privacy framework. Instead, the U.S. legislative framework for the protection of big data is a patchwork quilt of federal and state laws and regulations, common law, and industry self-regulation. The U.S. federal law takes a sectoral approach to privacy laws, imposing affirmative prohibitions and restrictions in certain commercial sectors. The top three sectors are financial, insurance and medical services. State laws add numerous additional privacy requirements. Privacy rights have also long been recognized and protected by common law in the United States. A network of common law torts, including invasion of privacy, public disclosure of private fact and remedies against general misappropriation or negligence serve to protect citizens’ rights to data privacy. Additionally, government agencies and industry groups have developed various guidelines that do not have the force of law but are considered “best practices” within particular industries and are often used as enforcement tools by regulators.

II. FINANCIAL SERVICES (FINANCIAL TECHNOLOGY AND INSURANCE)

In the United States, financial services constitute one of the most highly regulated sectors with regard to protection of nonpublic personal information (NPI) and personally identifiable information (PII). With major customer data

---

* Mr. Dehner is a member of Frost Brown Todd LLC and chairs the firm’s International Services Group. This article was prepared with the assistance of Molly F. McCartnery and Sunrita Sen.


2. See Leuan Jolly, Data Protection in United States: Overview, Practical Law Ctr. (July 1, 2016), Practical Law Country Q&A 6-502-0467.


breaches reported by the media on a regular basis, and identity theft as the fastest growing financial crime, regulators are focusing their attention on this growing issue. The regulatory landscape of the financial services sector, which includes financial technology and insurance, seeks to protect nonpublic personal information and personally identifiable information. Listed below are the relevant regulations that financial services institutions must observe, chief among which is the Gramm-Leach-Bliley Act of 1999.

A. Gramm-Leach-Bliley Act (GLBA)

Congress passed the Financial Services Modernization Act in 1999 (Gramm-Leach-Bliley Act or GLBA) to protect nonpublic personal financial information and ensure its security from unauthorized access. Similar to the EU Privacy Directive, GLBA requires that a financial institution “respect the privacy of its customers and protect the security and confidentiality of those customers’ nonpublic personal information.” GLBA separates individual privacy protection into two principal categories: (1) the Financial Privacy Rule and (2) the Safeguards Rule; both of which apply to “financial institutions.” According to the Federal Trade Commission (FTC), which enforces the provisions of GLBA, a “financial institution” is defined as any business, regardless of size, that is “significantly engaged” in providing financial products or services such as banks, securities firms, and insurance companies. Whether an institution is “significantly engaged” in financial activities to come under GLBA is a flexible standard that takes into account all facts and circumstances of the institution’s operations.

1. The Financial Privacy Rule

The Financial Privacy Rule (the “Privacy Rule”) applies to financial institutions that collect and receive nonpublic personal information from consumers, and requires them to disclose and provide a written notice of its policies and procedures to its customers. To be compliant with GLBA, a privacy notice must explain:

- the type of nonpublic personal information collected;
- the types of entities with whom the information is shared;
- how the information is used; and

---

6. See id.
8. See Jolly, supra note 2.
The privacy notice must also provide consumers with a reasonable opportunity to “opt-out” of any information sharing, if required by statute. Following this initial notice, financial institutions subject to GLBA must provide customers with an annual notice each year for as long as the customer relationship persists. In 2009, the federal financial regulators responsible for enforcing privacy regulations released model forms for financial institutions to use when developing their privacy notices pursuant to GLBA. Financial institutions that use the model form in a manner consistent with the regulators’ published instructions are deemed compliant with the regulation’s notice requirements.

2. The Safeguards Rule

The Safeguards Rule implemented pursuant to GLBA requires financial institutions to conduct a thorough risk assessment of security measures and design a comprehensive information security program to protect nonpublic personal information. Specifically, the Safeguards Rule requires financial institutions to “develop, implement, and maintain a comprehensive information security program” that contains administrative, technical, and physical safeguards designed to protect the security, confidentiality, and integrity of customer information. The statutory objective of the Safeguards Rule is to: (1) ensure the security and confidentiality of customer information; (2) protect against anticipated threats or hazards to the security or integrity of such information; and (3) protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer. An institution may exercise some latitude in developing its security program based on these objectives. While some critics may view this subjective standard as unenforceable, the FTC places a high level of responsibility upon financial institutions to keep up with the latest technology and the constant threat from potential identity thieves.

As part of the risk assessment, the Safeguards Rule requires an institution to:

- designate someone to coordinate the information security program;
- perform a thorough risk assessment and identify reasonably foreseeable internal and external risks to the security, confidentiality
and integrity of customer information that could result in unauthorized disclosure, misuse, alteration, destruction or other compromise of such information, and assess the sufficiency of any safeguards in place to control these risks.

Additionally, the Safeguards Rule requires an institution to design and implement information safeguards to control the risks identified and regularly test and monitor the effectiveness of the information security program’s key controls, systems and procedures.\(^{17}\) This duty also includes overseeing third-party service providers by taking reasonable steps to ensure that the service provider is capable of maintaining appropriate safeguards and requiring the service providers to agree contractually to implement and maintain such controls.\(^{18}\) The Safeguards Rule requires a financial institution to evaluate and adjust its information security program in response to its system test results or in response to any changes in its operations or business circumstances.\(^{19}\)

In brief, GLBA requires financial institutions to:

- provide notices of policies and practices regarding disclosure of personal information;
- prohibit the disclosure of such data to unaffiliated third parties unless consumers are provided the right to opt out of such disclosure or other exceptions apply; and
- establish safeguards to protect the security of personal information.

Noncompliance with GLBA may result in civil monetary fines of varying amounts up to $1 million or more; prison sentences of up to five years; lower examination ratings and increased reporting requirements; and enforcement actions, which can include board resolutions, memorandums of understanding, written agreements, and cease and desist orders. The specific action is based upon the number of deficiencies, risk profile, and whether or not violations have been encountered (such as transmitting unencrypted information to third parties, such as programmers, credit bureaus, loan processors, or other service providers).\(^{20}\)

**B. The Fair Credit Reporting Act (FCRA)**

The Fair Credit Reporting Act (FCRA), as amended by the Fair and Accurate Credit Transactions Act of 2003, imposes requirements on entities that possess or maintain consumer credit reporting information, or information generated from consumer credit reports. The FCRA mandates accurate and relevant data collection

---

17. See 16 C.F.R. § 314.4(c).
to give consumers the ability to access and correct their credit information, and limits the use of consumer reports to permissible purposes, such as employment and extension of credit or insurance.21 There is a private right of action for willful noncompliance, knowing noncompliance and negligent noncompliance with FCRA.22

C. Identity Theft and Assumption Deterrence Act

The Identity Theft and Assumption Deterrence Act of 1998 was created to address the growing problem of identity theft in the U.S. by regulating: 1) the fraudulent creation, use or transfer of identification documents, and 2) the theft and/or criminal use of the underlying personal information. It applies to anyone who knowingly transfers or uses NPI or PII with the intent to commit, or aid and abet any unlawful activity. While identity theft can occur through a variety of means, unprotected electronic communications are a primary target. Therefore, electronic communications should be subject to content monitoring and filtering to lessen the potential for data leakage through these network channels. Violations of the Act are generally subject to a fine and/or imprisonment of up to 15 years. Specifications are determined at the time when the infraction is reported or during a regulatory examination.23

D. The USA Patriot Act

Section 314 of the Patriot Act requires financial institutions to implement prudent steps to protect the confidentiality of NPI. Proactive monitoring and auditing of electronically transmitted information is required for alerting organizations to: unauthorized access, unauthorized sharing or other compromises of protected information. The integrity and protection of NPI is imperative for the monitoring and investigation of money laundering and terrorist financing. Fines in an amount not more than 3 times the monetary equivalent of the thing of value, or imprisonment up to 15 years, or both may be assessed for violations of this Act.24

E. Sarbanes-Oxley Act

Section 404 of the Sarbanes-Oxley Act of 2002 mandates that publicly traded companies implement and maintain internal controls for the protection of corporate financial information, and for the timely detection of unauthorized access, insider abuse and unauthorized sharing of the information. Organizations found to be noncompliant are subject to fines of up to $1 million and sentences of up to 10 years in prison.25

22. 15 U.S.C. §§ 1681n(a)-(b), 1681o(a).
F. EU-U.S. Privacy Shield Framework

The EU-U.S. Privacy Shield Framework replaced the U.S.-EU Safe Harbor Program in February 2016. It provides a method for companies to transfer personal data to the United States from the European Union (EU) in a way that is intended to be consistent with EU law. The agreement contains three key features:

1. Strong Obligations for Companies’ Handling of EU Citizens’ Data

To join the Privacy Shield Framework, a company must self-certify to the Department of Commerce that it complies with the Privacy Shield Principles. A company’s failure to comply with the Principles is enforceable under Section 5 of the FTC Act prohibiting unfair and deceptive acts.

III. Medical Services

A. HIPAA

Title II of the Health Insurance Portability and Accountability Act (HIPAA) of 1996 required the adoption of federal privacy and security protections for Protected Health Information (PHI). PHI is individually identifiable health information that relates to an individual’s care, health status or payment of care, that identifies the individual. To implement HIPAA, the U.S. Department of Health and Human Services (HHS) issued the HIPAA Privacy Rule and the HIPAA Security Rule. HHS also enacted a Breach Notification Rule and an Enforcement Rule. Covered Entities (CEs) and their Business Associates (BAs) (collectively, Entities) must comply with the Privacy and Security Rules. CEs are: health care providers who transmit health information electronically; health care clearinghouses; and health plans. CEs include doctors, nursing homes, pharmacies, and health insurance companies. BAs are entities that have access to or use PHI in the course of performing specified functions or services on behalf of a CE.

The Privacy and Security Rules do not govern information that is de-identified, patient-generated, or in a non-covered entity’s possession. PHI may be de-identified by removing 18 identifiers, such as name and social security number. Once de-identified, the information may be used and disclosed without restriction.

27. 45 C.F.R. § 160.103.
28. 45 C.F.R. § 160.103.
HIPAA does not govern patients and therefore does not protect patient-generated health data submitted to non-covered entities, such as websites like PatientsLikeMe.com, that collect individual’s health information to sell.30

1. Privacy Rule

The Privacy Rule establishes standards to protect PHI. The Rule: (a) governs how and when PHI can be used and disclosed; (b) identifies the rights an individual has regarding their PHI; and (c) establishes additional administrative requirements.31

(a) Use and Disclosure of PHI

The rules for collection, use and disclosure32 of PHI under the HIPAA Privacy Rule vary based on the purpose for which the information is collected or used. Generally, regulated entities are prohibited from using or disclosing PHI without the signed authorization of the patient. For example, authorization is required to use or disclose psychotherapy notes and to use or disclose PHI for marketing purposes.33 However, the Privacy Rule permits entities to use and disclose PHI without first obtaining a patient’s authorization if it is in accordance with the following permitted use and disclosure exceptions: 34

- Treatment, payment and health care operations.35
- Public health functions. PHI may be disclosed for purposes related to preventing or controlling disease, injury or disability.36
- Limited datasets. Regulated entities may disclose a limited dataset for research, public health or health care operations. A limited dataset is stripped of 16 specified identifiers.37 The parties must enter into a data use agreement that outlines the

---

32. A disclosure is defined as the release, transfer, provision of access to or divulging in any other manner information outside the entity holding the information. 45 C.F.R. § 160.103.
33. HITECH Act, § 13405(d); 45 C.F.R. § 164.508; 78 Fed. Reg. at 5606.
34. 45 C.F.R. § 164.502(a).
35. 45 C.F.R. § 164.506. See 45 C.F.R. § 164.501 for activities that qualify as “health care operations.”
36. 45 C.F.R. § 164.512(b)(1)(i)-(vi).
37. 45 C.F.R. § 164.514(e).
specific permitted uses of the PHI, including who can use the PHI.\textsuperscript{38}

- Other exceptions under the Privacy Rule include law enforcement purposes, or research if an institutional review board has waived the authorization requirement.\textsuperscript{39}

Under the Privacy Rule, a CE or BA must make reasonable efforts to use, disclose, and request only the minimum amount of PHI needed to accomplish the intended purpose of the use, disclosure, or request.\textsuperscript{40}

(b) Individual Rights
An individual’s right to the person’s health information includes a right to: \textsuperscript{41}

- Receive a Notice of Privacy Practices. The notice must describe how the entity may use and disclose PHI; state the entity’s privacy practices and legal duties to protect privacy; and specify the individual’s rights with respect to PHI.\textsuperscript{42}
- Access and obtain a copy of one’s own PHI.\textsuperscript{43}
- Amend one’s PHI.\textsuperscript{44}
- Confidential communications.\textsuperscript{45}
- Restrict uses and disclosures of their PHI.\textsuperscript{46}

(c) Administrative Requirements\textsuperscript{47}
A CE must adopt and implement privacy procedures that minimize the amount of PHI used, disclosed, and requested; train employees on the privacy procedures; and have procedures for individuals to complain about a CE’s noncompliance with its privacy policies or the Privacy Rule. A CE must maintain reasonable and appropriate administrative, technical, and physical safeguards that limit use or disclosure and prevent use or disclosures in violation of the Privacy Rule. Examples of safeguards include securing medical records with a lock and

\textsuperscript{38} How Does the HIPAA Privacy Rule Apply to Research?, HEALTH INFORMATION & THE LAW (June 2014), http://www.healthinfolaw.org/article/fast-facts-how-does-hipaa-privacy-rule-apply-research.

\textsuperscript{39} 45 C.F.R. § 164.512(a)(c)–(l).

\textsuperscript{40} 45 C.F.R. §§ 164.502(b), 164.514 (d).


\textsuperscript{42} 45 C.F.R. § 164.520.

\textsuperscript{43} 45 C.F.R. § 164.524.

\textsuperscript{44} 45 C.F.R. § 164.526.

\textsuperscript{45} 45 C.F.R. § 164.522(b)(1).

\textsuperscript{46} 45 C.F.R. § 164.522.

shredding documents before discarding them. A CE must mitigate any harmful effect caused by the use or disclosure of PHI in violation of the Privacy Rule.

2. Security Rule

The Security Rule establishes security standards for protecting electronic PHI (ePHI). The Security Rule does not apply to PHI transmitted orally or in writing.\(^{48}\) The Security Rule requires CEs and BAs to adopt administrative, physical and technical safeguards to protect ePHI it creates, receives, maintains or transmits.\(^{49}\)

a) Administrative Safeguards.

These safeguards include requiring Entities to: \(^{50}\)

- conduct regular security risk analyses and implement security measures to reduce risks;
- designate a security official to develop and implement security policies and procedures;
- create policies and procedures to limit access to ePHI to only those workforce members whose duties make it appropriate to have access; and
- train all workforce members on security issues, policies, and procedures.

b) Physical Safeguards.

These safeguards include requiring Entities to: \(^{51}\)

- limit physical access to its facilities;
- specify the proper use of and access to workstations and electronic media; and
- establish policies and procedures for the transfer, removal, disposal and re-use of electronic media.

c) Technical Safeguards.

These safeguards include requiring Entities to implement: \(^{52}\)

- hardware, software, and procedures to record and examine activity in information systems that contain or use PHI;
- policies and procedures that protect ePHI from improper modification or destruction;
- policies and procedures to verify that persons seeking access to ePHI are who they claim to be; and

---

48. *Id.*
49. 45 C.F.R. § 164.530(c).
50. 45 C.F.R. § 164.308(a).
51. 45 C.F.R. § 164.310.
52. 45 C.F.R. § 164.312(b-e).
• policies and procedures that prevent unauthorized access to ePHI being transmitted over an electronic communications network.

d) Other Requirements. Entities must:

• take reasonable steps to cure a breach if the entity knows of an activity or practice of a business associate that constitutes a material breach; 53

• obtain Business Associate Agreements from their BAs; 54

• implement reasonable and appropriate policies and procedures to comply with the Security Rule; 55

• keep documents for six years after the later of the creation date or last effective date; 56 and

• periodically review and update its documentation to ensure the confidentiality, integrity, and availability of ePHI. 57

3. Breach Notification Rule

A CE must provide notice, after the discovery of a breach of unsecured PHI, to affected individuals and HHS. 58 A BA of a CE that accesses, maintains, retains, modifies, records, destroys, or otherwise holds, uses, or discloses unsecured PHI must notify the CE when it discovers a breach. 59 A CE must provide breach notification to prominent media outlets in a state, if the breach involves more than 500 residents of the state. 60

A breach is an unauthorized acquisition, access, use, or disclosure of PHI that compromises PHI’s security or privacy. 61 An impermissible acquisition, access, use, or disclosure of PHI is presumed to be a breach unless a CE or BA demonstrates that there is a low probability that the PHI was compromised, based on a risk assessment. 62 Uses or disclosures that impermissibly involve more than the minimum necessary information may qualify as breaches.

53. See 45 C.F.R. § 164.314(a)(1).
54. Id.
55. 45 C.F.R. § 164.316.
56. Id.
57. 45 C.F.R. § 164.316(b)(2)(iii).
58. 45 C.F.R. § 164.404(a); 45 C.F.R. § 164.408(a).
59. 45 C.F.R § 164.410(b).
60. 45 C.F.R. § 164.406(a).
61. 45 C.F.R. § 164.402.
62. 45 C.F.R. § 164.402(2).
4. Enforcement Rule

The Office of Civil Rights (OCR) is responsible for enforcing the Privacy and Security Rules. An individual who believes an Entity is not complying with HIPAA may file a complaint. OCR investigates filed complaints, and conducts compliance reviews to investigate alleged violations brought to its attention by means other than complaints. HIPAA may also audit Entities to review their policies and procedures. OCR imposes civil monetary penalties if it determines that an Entity has violated HIPAA. Penalties range from $100 to $50,000 per violation but cannot exceed $1.5 million for identical violations during a calendar year. A violation may also be subject to criminal penalties.

OCR may enter into resolution agreements with CEs to settle violation complaints. Resolution agreements generally require the CE to make a payment, which has ranged from $35,000 to over $2 million. Most agreements waive a CE’s appeal rights, provide that the CE cannot contest the validity or amount of the payment, and require CEs to comply with certain obligations and make reports to OCR. For example, in 2013, OCR announced a $1.2 million settlement with a health plan after an investigation, resulting from a breach notification, revealed the health plan had impermissibly disclosed ePHI of over 300,000 individuals by failing to erase photocopier hard drives before returning the photocopiers to a leasing company.

B. HITECH Act and GINA

In 2013, HHS issued a Final Omnibus Rule that updated HIPAA to reflect changes required by the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009 and the Genetic Information Nondiscrimination Act (GINA) of 2008.

64. 45 C.F.R. § 16.306. HIPAA does not have private cause of action. Dodd v. Jones, 623 F.3d 563, 569 (8th Cir. 2010).
67. See 45 C.F.R. § 160.404(b).
70. 42 U.S.C. § 17930, et seq.
1. HITECH Act

The HITECH Act modified HIPAA’s Privacy, Security and Enforcement Rules and established the Breach Notification Rule.\(^{72}\) The act expanded the definition of “business associates” to include subcontractors and established that business associates of covered entities are directly liable for compliance with certain HIPAA Privacy and Security Rule requirements.\(^{73}\) Modifying the Enforcement Rule, the act increased the penalties for HIPAA violations.\(^{74}\) Changes to the Privacy Rule included prohibiting the sale of PHI without an individual’s prior written authorization and amending the Notice of Privacy Practices requirements. New statements required by the Notice of Privacy Practices included explaining the uses and disclosures that require prior authorization.\(^{75}\) The act also mandated the adoption of the Breach Notification Rule that governs an entity’s responsibilities for unauthorized disclosures of unsecured PHI.

2. GINA

GINA’s added privacy protections for genetic information required changes to the HIPAA Privacy Rule to clarify that PHI includes genetic information and is therefore protected under the HIPAA Privacy Rule.\(^{76}\)

C. 42 C.F.R. Part 2

42 C.F.R. Part 2, the Confidentiality of Alcohol and Drug Abuse Patient Records (Part 2) regulation, restricts the disclosure and use of patient identifying information of individuals in federally assisted substance abuse treatment.\(^{77}\) Patients must provide written consent to disclose information that could identify them as having a current or past substance abuse problem.\(^{78}\) Unlike HIPAA, which generally permits the disclosure of PHI for the purposes of treatment, payment, or health-care operations, Part 2 is more prohibitive because it requires patient

---


\(^{74}\) *Id.*


\(^{78}\) 42 C.F.R. §2.12(a); *Frequently Asked Questions*, supra note 77.
consent for such disclosures. Limited exceptions to consent include medical emergencies.

D. State Laws

HIPAA provides a floor of federal protections for PHI. But CEs and BAs may also be subject to state privacy laws that address the protection of PHI. Although HIPAA preempts contrary state laws, it does not preempt state laws that are more stringent than the HIPAA requirement. For example, the California Confidentiality of Medical Information Act provides for a private right of action unlike HIPAA, and while HIPAA provides 30 days to respond to patient access requests, the California Patient Access to Health Records Act provides that patients are entitled to inspect their records within 5 business days of the request. Because these California laws provide for greater protections than HIPAA, they are not preempted.

IV. INSURANCE

Recently reported cyber-attacks on Anthem Inc., Premera Blue Cross, and Care First BlueCross BlueShield illustrate that all aspects of the financial sector are targets and potentially vulnerable to cyber-attack. Insurers, in particular, are data-rich targets for cyber attackers. For this reason, insurers are scrutinized and held to the same nationally rigorous regulatory standards for data privacy as other financial institutions. The Financial Services Modernization Act of 1999, also known as Gramm-Leach-Bliley, includes provisions for state insurance authorities to establish appropriate standards “relating to administrative, technical, and physical safeguards – (1) to insure the security and confidentiality of customer records and information; (2) to protect against any anticipated threats or hazards to the security and integrity of such records; and (3) to protect against unauthorized

79. Frequently Asked Questions, supra note 77.
80. 42 C.F.R. §2.51(a).
82. 45 C.F.R. § 160.203(b).
83. 45 C.F.R. § 164.524(b)(2).
84. CAL. HEALTH & SAFETY CODE § 123110.
access to or use of such records or information which could result in substantial harm or inconvenience to any customer.\footnote{89} In response, the National Association of Insurance Commissioners developed two model regulations: (1) the Privacy of Consumer Financial and Health Information Regulation, which governs treatment of nonpublic personal health information and nonpublic personal financial information (NPFI) by licensees; and (2) Standards for Safeguarding Consumer Information Model Regulation, which establishes standards for developing and implementing administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer information. All 50 states and the District of Columbia have adopted the Privacy of Consumer Financial and Health Information Regulation, or a substantially similar regulation. 36 states have adopted some version of the Standards for Safeguarding Consumer Information Model Regulation, or a substantially similar regulation.

The Federal Financial Institutions Examination Council (FFIEC)’s Cybersecurity Assessment Tool (Assessment) has been developed to provide a uniform examination standard for cyber security oversight to be used internally by a financial institution’s senior management and board of directors.\footnote{90} The Assessment can also be a valuable tool for regulatory oversight of data privacy by state insurance regulators. Additionally, the National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity (NIST Cybersecurity Framework) provides a voluntary blueprint that firms of all sizes can use to evaluate, maintain, and improve the resiliency of computer systems and reduce cyber risk. The Federal Insurance Office of the United States Department of Treasury has encouraged insurers and other financial services firms to implement the NIST Cybersecurity Framework.\footnote{91}

Health insurers are subject to HIPAA regulations. The HIPAA Privacy and Security Rules regulate the use, disclosure and security of protected health information (PHI) by covered entities (CEs). Health plans are a type of CE, which includes insurance companies, HMOs, company health plans, and government programs that pay for health care such as Medicaid and Medicare.\footnote{92} Additionally, the Genetic Information Nondiscrimination Act (GINA) impacts health insurers. After GINA added privacy protection requirements for genetic information, the HIPAA Privacy Rule was modified to prohibit health plans from using or disclosing genetic information to make health insurance coverage-related decisions and from requesting that beneficiaries undergo genetic testing or provide genetic information.\footnote{93} The prohibited use for underwriting purposes includes: eligibility determinations, premium computations, applications of any pre-existing

\footnote{89. 15 U.S.C. § 6801(b).}
\footnote{90. See Cybersecurity Assessment Tool, FED. FIN. INST. EXAMINATIONS COUNCIL (October 17, 2016), https://www.ffiec.gov/cyberassessmenttool.htm.}
\footnote{92. 45 C.F.R. § 160.103.}
\footnote{93. Genetic Information, supra note 76.}
condition exclusions, or for any other purpose related to the creation, renewal, or replacement of health insurance or health benefits.

In 2014, state insurance regulators established a Cyber Security Task Force to coordinate insurance regulatory activities relating to cyber security issues, including analyzing information regarding the cyber insurance market and discussing potential regulatory standards relating to cyber security. On April 16, 2015, state insurance regulators released Principles for Effective Cybersecurity Insurance Regulatory Guidelines—12 guiding principles to assist states in developing regulatory regimes intended to protect consumers and the insurance industry from cyber threats. Additionally, state insurance regulators on the NAIC’s Property and Casualty Committee released its Cybersecurity Blanks proposal, which would require submission of additional annual statement information regarding cyber insurance issued as stand-alone coverage or as part of commercial multi-peril policies, including premiums, losses, direct defense and cost containment, and number of policies in force.95

In February 2015, the New York Department of Financial Services (NYDFS) issued the Report on Cyber Security in the Insurance Sector, following a survey of a cross-section of regulated insurance companies. The NYDFS, leading the national effort among state insurance regulators, determined that enhanced supervisory cyber security examinations are necessary in order to identify vulnerabilities in insurers and to identify appropriate solutions. Insurance regulators from other states, including Alaska, California, Indiana, Maine, Missouri, New Hampshire, North Dakota, Oregon, South Carolina, and Washington, are conducting multi-state market conduct examinations of Anthem and Premera. These examinations focus on the events affecting Anthem and Premera, the insurers’ cyber security protections that had been in place, the impact of the security breaches on consumers, and the measures the insurers have taken to prevent unauthorized access to or losses of data that could result from future attacks.98

TRENDS FOR POTENTIAL INSURANCE COVERAGE FOR LOSSES ARISING FROM A DATA BREACH

Nathan L. Colvin* and Timothy C. Dougherty**

I. INTRODUCTION

The costs arising out of data breaches—including monetary damages, lawsuits, fines and the like—are increasing for victims—especially large companies.¹ Consequently, companies have increasingly sought insurance coverage for damages and costs flowing from a breach, under both existing and prospective policies. This article will discuss trends in the ability of companies to obtain such coverage under existing policies, as well as the scope of such coverage that companies should consider when purchasing a policy.

More specifically, this article will first discuss attempts by companies to obtain coverage for breaches under traditional insurance policies, such as commercial general liability policies. Second, this article will discuss the insurance industry’s response to such efforts, including the creation of special cyber liability policies for data breach losses. And finally, this article will discuss legal issues and potential areas of future dispute arising out of such specialty policies.

II. EARLY ATTEMPTS TO OBTAIN COVERAGE THROUGH COMMERCIAL GENERAL LIABILITY INSURANCE

Initially, companies facing financial losses resulting from a data breach have looked to their commercial general liability (“CGL”) policies for coverage. Like homeowners insurance for a homeowner, CGL policies are held by most companies and insure against general business risks, such as bodily injury or property damage on company premises, damage caused as part of company operations, or damage caused by the company’s employees. In the context of data breaches, companies have sought coverage for the tangible loss of use of property or for “personal and advertising injury” suffered by the company’s employees or customers, both of which are types of coverage typically found in CGL policies. The results of these legal efforts have been mixed.

---


* Mr. Colvin is a litigation associate at Vorys, Sater, Seymour and Pease LLP, where he has counseled clients regarding insurance coverage both before and after a data breach.

** Mr. Dougherty is a litigation associate at Vorys, Sater, Seymour and Pease LLP.
A. Loss of Tangible Property

One potential opportunity for coverage has been for loss of tangible property, resulting from a data breach. Specifically, companies have argued that the loss of use of computers, systems, or data due to breaches or hacking could constitute “tangible property damage” covered by commercial general liability policies. For example, in State Auto Pro. & Cas. Ins. Co. v. Midwest Computers & More, the district court held that coverage was available for loss of tangible property where the corporate computers were corrupted by a virus and the damage rendered the computers totally unusable. Judicial interpretation of the word “tangible,” however, has resulted in limits to the extent of such coverage. In reality, the most significant damages flowing from a data breach relate to the loss or compromise of the data itself—and all of the damages flowing from that loss, such as lawsuits, fines, and the like—rather than the loss of use of hardware. While courts have been willing to view hardware as “tangible property,” the same has not been the case for data. In Am. Online Inc. v. St. Paul Mercury Ins. Co., for instance, the federal court held that “[c]omputer data, software and systems are incapable of perception by any of the senses and are therefore intangible.” Consequently, the tangible property loss theory of coverage has been of limited consequence in a typical data breach case.

B. Personal and Advertising Injury

Companies have had more success pursuing data breach claims under the theory of personal and advertising injury. This theory invokes policy language that typically covers injuries arising out of “oral or written publication in any manner, of material that violates a person’s right to privacy.” Traditionally, the purpose of this type of CGL coverage was to provide coverage for instances where a company is accused of defaming an individual, or using an individual’s information or likeness in advertising without permission. In the data breach context, the focus of the courts has been on the manner of publication.

In Recall Total Info Mgmt. v. Fed. Ins. Co., for example, the Connecticut Supreme Court found that publication did not occur in a case in which tapes containing data for 500,000 IBM employees fell out of a van operated by a transportation company. As a result of the incident, IBM suffered losses relating to its purchase of identity protection coverage for its employees. IBM sought

---

3. Id.
7. See Id. at 49.
reimbursement from the transportation company who, in turn, sought coverage from its insurer.\(^8\) Although the company was unable to ever find the tapes—suggesting that someone else found them—the Connecticut Supreme Court ultimately held that there was no personal and advertising injury because there was no evidence that the tapes were ever accessed, meaning that there was no actual “publication” of the information contained on the tapes.\(^9\)

In *Travelers Indem. of Am. v. Portal Healthcare*, the insurance made a similar—but this time unsuccessful—argument that publication did not occur.\(^10\) In that case, individual medical records were uploaded to a publicly accessible internet site, but there was no evidence that the records were ever accessed by a third party.\(^11\) Without evidence that the data was viewed, the insurance company argued that publication of data had not occurred.\(^12\) The court disagreed, holding that “[p]ublication occurs when information is ‘placed before the public,’ not when a member of the public reads the information placed before it . . . [T]he medical records were published the moment they became accessible to the public via an online search.”\(^13\)

There is some tension between these two cases in that, in both instances, data was arguably “accessible” to the general public because someone could have found (and likely did find) the IBM data tapes, just as someone could have found (but apparently did not find) the health records online. The clear upshot of these cases is that companies seeking coverage for a personal advertising injury will need to establish that data was either actually viewed or was generally accessible to the public.

At least two further challenges exist when a company seeks coverage for data breach damages through personal and advertising injury coverage. First, in many cases, data is encrypted. There may be an argument that, although the data was accessed and in some sense viewed, the viewer would not have been able to discern personal and private information. In fact, a company facing consumer class actions may have strong reason to argue that the class suffered no injury because the data was encrypted and there is no evidence that the hackers actually broke the encryption.

Second, while it is clear that coverage exists where the company or its employees “publish” data, what about when a hacker gains access to the data? Has the company “published” the data once it becomes accessible to the hacker? Does coverage exist where the hacker—who is not an employee of the company—is the one publishing the data? The court in *Zurich Am. Ins. v. Sony*

---

8. See *Id.* at 49-50.
9. *Id.* at 50-51 (citing 147 Conn. App. at 462-65).
11. *Id.* at 770-71.
12. *Id*.
13. *Id.* at 771.
Corp of Am. dealt with this question in the aftermath of the hack of Sony’s data.14 There, the Court rejected Sony’s argument that coverage for publication “in any manner” should include publication by a hacker, concluding that such language was limited to publication in “any manner” by Sony—not by third parties.15 While Sony appealed the ruling, the parties ultimately settled.16 The court also did not endorse Sony’s argument that the hackers accessing Sony’s systems amounted to an unintentional or negligent publication of data by Sony.17

III. THE INSURANCE INDUSTRY RESPONDS TO RISING DATA BREACHES

Despite the mixed bag of results for coverage under CGL policies, the insurance industry has responded to the increase in data breaches and corresponding claims for coverage by beginning to exclude coverage under CGL policies. Insurers would, of course, argue that CGL policies (and personal and advertising injury coverage especially) were never intended to provide coverage for data breaches. And in light of the growing risks of claims and exposure for data breaches, many insurers have begun to exclude coverage in CGL policies.

Specifically, the Insurance Services Office (“ISO”), which drafts standard language for adoption by insurers, has revised its standard CGL policy language to specifically exclude coverage for damages caused by data breaches. These exclusions in turn have been popularly adopted by insurers. For example, many CGL policies now provide that coverage for tangible loss of use of property does not cover the access or disclosure of personal information. Likewise, many policies now provide that access or disclosure of personal information is not a defined injury within personal and advertising injury coverage. Consequently, there will be fewer and fewer attempts to obtain coverage for data breaches under CGL policies.

Companies should not despair, however, because the insurance industry recognized the need for insurance coverage for data breaches. Increasingly, insurance companies offer riders or separate cyber liability policies specifically underwritten for these risks.18 Such policies typically provide coverage for various consequences flowing from a data breach, including coverage for investigations, lawsuits, the provision of identity protection services, reputational harm, and consequential damages.19 In some cases, these policies even provide for coverage to pay a ransom if a hacker locks a company out of its own systems.20

---

15. Id. at *68-72.
19. Id.
Despite the apparent comprehensiveness of these policies, companies would be mindful to review such policies for potential limitations in coverage. Because these policies are relatively new, litigation over such limitations has just begun.

Recent litigation flowing from the data breach of the restaurant chain P.F. Chang’s illustrates this. In *P.F. Chang’s v. Fed. Ins. Co.*, P.F. Chang’s sought coverage for $1.9 million it paid in assessments to a payment card processing company. By way of background, merchants that wish to accept payment cards (Visa, MasterCard, etc.) enter into agreements with payment card processing companies. These contracts typically contain provisions that require the merchant to indemnify the payment card processing company for any damages or liabilities that might arise out of their relationship, including any flowing from a breach of the merchant’s systems. In turn, the payment card processors are similarly contractually bound to pay for any damages relating to a breach of their customer’s systems if the merchant is not in compliance with the Payment Card Industry Data Security Standards, which govern the security measures that must be in place for merchants that accept payment by payment card brands. Consequently, when a merchant suffers a breach, significant fines, assessments and other costs can be assessed by the payment card brands on the payment card processor who then seeks indemnification from the merchant.

At issue in *P.F. Chang* was whether the cyber liability policy provided coverage for this indemnification. The insurer denied the claim because the policy excluded losses arising out of contractual obligations to third parties—which is a common exclusion in insurance policies. Although the contractual obligation arose out of a data breach, the Court agreed that the policy exclusion applied because the root of the obligation to pay the $1.9 million was contractual indemnification. This was despite the fact that the policy would have generally covered those types of fines if they had been levied directly on P.F. Chang’s by the payment card brands.

The perhaps obvious takeaway from *P.F. Chang*’s is to carefully review the entire policy, including the exclusions, for potential inconsistencies. In many

---

(discussing coverage options for ransom payments); Patrick Nelson, “Why companies are becoming more likely to pay when struck by ransomware,” NETWORKWORLD, Feb. 15, 2016, available at: http://www.networkworld.com/article/3032554/security/why-companies-are-becoming-more-likely-to-pay-when-struck-by-ransomware.html (discussing study showing increased likelihood companies will pay ransom due to insurance coverage).

22. Id. at *6.
23. E.g., id. at *4.
24. E.g., id. at *3-4.
25. E.g., id. at *4-6.
26. Id. at *6-7, 11.
27. Id. at *21-22.
28. Id. at *24.
29. Id. at *23-24.
cyber-liability policies, the exclusion at issue in *P.F. Chang* makes clear that it does not apply to assessments levied by payment card brands.

There are other potential exclusions of coverage that are likely to lead to disagreements in the coming years. One such potential exclusion is for claims arising out of the acts of independent contractors. Such exclusions could potentially loom large, as it is not uncommon for a hacker to gain access to a company’s systems through the use of a third-party vendor’s credentials. For example, the 2013 breach of Target, which led to more than $100 million in settlements, was believed to have been accomplished through an independent contractor’s credentials.\(^\text{30}\) Similarly, it is not unusual for a company insider to be involved in a data breach, and many policies exclude coverage for the intentional and wrongful acts of employees.

An additional potential roadblock to coverage is the common exclusion of coverage for injuries flowing from acts of a foreign state or acts of terrorism. Ordinarily, coverage is available for losses caused by the criminal acts of third parties.\(^\text{31}\) But recall that the hack of Sony Pictures Entertainment around the projected release of the motion picture *The Interview* was widely believed to have been sponsored by the North Korean government as retribution for the film’s planned release.\(^\text{32}\) The hack included the release of personal information about Sony Pictures employees and their families that led to litigation.\(^\text{33}\) It is not hard to imagine an argument that claims flowing from a hack sponsored by a foreign government would be subject to such exclusion.

### IV. Conclusion

Unquestionably, the terms and judicial interpretations of insurance policies will continue to develop as the number of significant data breaches continues to climb, leading to more and more claims by the victims of data breaches. All companies—but especially those that are susceptible to significant breaches—would do well to continue to monitor these developments to ensure that coverage is available in the event of a breach.

---


MERCHANT LIABILITY TO FINANCIAL INSTITUTIONS FOR A DATA BREACH

J.B. Lind*, et al.

I. INTRODUCTION

Credit card breaches are becoming more and more common place. Over the last decade, merchants in almost all business sectors have faced such breaches including Neiman Marcus, Target, Wendy’s, Home Depot, Blue Cross, Kmart, Staples, and many others. When such breaches occur, merchants can face significant liability. This article will discuss two potential sources of merchant liability to financial institutions flowing from a data beach. First, the article will discuss the fines and assessments brought by the Payment Card Industry (“PCI”) under the contractual infrastructure that governs credit card transactions. And second the article will discuss class action lawsuits brought by the financial institutions that bear the costs of card replacement and fraud. As is discussed in further detail below, liability arises in both instances from banks. From the merchant’s contract with its own bank (the “acquiring bank”), in the first instance, and from the compromised cardholder’s financial institution (the “issuing bank”) in the second instance.

II. MERCHANTS ARE CONTRACTUALLY OBLIGATED TO INDEMNIFY THEIR ACQUIRING BANKS FOR FINES AND ASSESSMENTS LEVIED BY THE PAYMENT CARD INDUSTRY

In 2006, the five major credit card brands—American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa, Inc.—joined together and formed the Payment Card Industry Security Standards Council ("PCI SSC") for the purpose of managing the evolution of PCI Data Security Standard ("PCI DSS"). These efforts were designed to combat the fraud occurring as a result of internet sales. The card brands agreed to incorporate the PCI DSS as the technical requirements of their data security compliance programs. The PCI SSC periodically revises and updates the PCI DSS, which are currently comprised of twelve significant requirements, including sub-requirements and numerous directives related to data security.2

* Mr. Lind is a partner in the Vorys Cincinnati office and a member of the litigation practice group. J.B. has a broad range of litigation experience including business, commercial, construction, insurance, product liability/toxic tort, probate/estate litigation, intellectual property litigation and information privacy/data breach litigation.


The PCI DSS are incorporated into the membership agreements between the credit card associations and the acquiring banks—the agreements which enable the bank to utilize the card brands. The membership agreements also obligate the acquiring banks to pay any fines or assessments levied by the PCI for violation of those standards. The PCI DSS are, in turn, incorporated into merchants’ agreements with their acquiring banks.

Merchants will enter into a merchant services agreement with an acquiring bank in order to accept credit card payments. These agreements incorporate the PCI DSS and obligate merchants to indemnify the acquiring bank for any PCI assessments and fines levied against the acquiring bank as a result of the merchant’s noncompliance with PCI DSS and the data breaches that result. This contractual infrastructure is meant to help facilitate recovery from merchants of fraud and card reissuance expenses incurred by the payment card brands, who are not otherwise in privity of contract with merchants.

A. Noncompliance Fines

Fines are punitive in nature and are levied for PCI noncompliance. Acquiring banks are responsible for enforcing compliance and typically do so one of two ways: (1) providing merchants with a self-reporting checklist; or (2) requiring the merchant to undergo a full audit by a certified third-party security expert. The style of compliance demonstration required is determined entirely by the acquiring bank. The fines can range from a few thousand dollars a month up to hundreds of thousands of dollars depending on the severity of the noncompliance.

B. Operational and Fraud Assessments

Assessments differ from noncompliance fines in that they do not come into play until an actual data breach occurs. They are the primary means by which an issuing bank can recover losses sustained as a result of a data breach. An assessment occur when a breach leads to fraudulent credit card use and are an attempt to reimburse the issuing banks for the cost the fraudulent transactions and for reissuing cards. Before an assessment is levied, certain minimum threshold requirements must be met. For example, VISA requires that 15,000 cards be potentially at risk and there is at least $150,000 in combined operating and fraud recovery. The basis for an assessment is the report generated by a PCI Forensic Investigator (“PFI”), who is called in to determine the extent of a data breach and how it may have occurred. Some critics believe that PFIs are generally aligned with the card brands and have leeway to make certain assumptions such as how long the breach continued (which increases the number of potential cards at risk). Merchants can affect this process by hiring their own investigator to influence the outcome of the PFI’s report, which can involve a significant expense for the merchant.
There are two types of assessments: Operating Expense Assessments and Fraud Assessments. The former is essentially a formula that multiples the number of cards deemed to be compromised by a given value. For example, VISA uses a sliding scale for costs associated with card replacement based upon the issuer’s size with smaller institutions receiving a higher amount per card than larger institutions. Fraud recovery assessments are highly variable and dependent on the nature of the breach. The amounts are based on the PFI’s investigation and, once the report is issued, there is very little recourse available to merchants.

C. Case Illustration: Genesco, Inc. v. Visa U.S.A., Inc.

The facts in Genesco, Inc. v. Visa U.S.A., Inc. provide an illustration of how this arrangement plays out and the types of fines and assessments that are levied against a merchant. In 2010, Genesco suffered a cyberattack. VISA identified the potential breach when it discovered that multiple issuer banks reported fraudulent activity with Genesco-owned stores as the common point of purchase. VISA required the acquiring banks to validate Genesco’s compliance and a PFI conducted a forensic examination, which ultimately found the Genesco was noncompliant on three of the twelve PCI DSS requirements. Based on the report, VISA assessed Genesco’s acquiring bank over $13 million for fraud and operating expense assessments. Under Genesco’s agreements with its acquiring banks, it was required to indemnify them for any such fines and assessments. Ultimately, Genesco brought suit against VISA. Presumably, the parties settled as the case was dismissed before a decision on the merits.

While Genesco successfully survived VISA’s motion to dismiss, this layered contractual arrangement makes the merchant ultimately liable for the fines and assessments, while providing insulation to the credit card brands from claims that the fines and assessments are inappropriate. This was recently illustrated in the case of Jetro Holdings, LLC v. Mastercard Intl., Inc. There, after data breaches were discovered, MasterCard levied two fraud recovery assessments totaling nearly $7 million against PNC, Jetro’s acquiring bank. PNC passed the assessment on to Jetro through its merchant services agreement. Jetro brought suit against MasterCard for breach of contract, breach of good faith and fair

---

4. Id. at 562.
5. Id. at 563.
6. Id.
7. Id. at 564.
8. Id. at 561.
10. Id. at *2.
11. Id.
dealing and unjust enrichment. MasterCard, however, argued that Jetro lacked standing to sue it because the two were not in privity of contract. Jetro argued in response that, because its acquiring bank withheld Jetro’s funds to pay MasterCard, Jetro should be equally subrogated to the rights of the acquiring bank to seek recoupment from MasterCard of funds MasterCard wrongfully collected. The court rejected this argument. Relying on the language of the contract between Jetro and PNC, the court found nothing inequitable about Jetro being forced to bear the assessments costs. The decision is currently on appeal and, if affirmed, could put merchants in a difficult spot if they wish to challenge the assessments that are passed down by the payment card brands.

III. ISSUING BANKS BRING SUIT TO RECOVER DAMAGES RESULTING FROM DATA BREACHES

While assessments are meant to reimburse issuer banks for the costs associated with replacement of compromised cards and fraud, issuer banks are also bringing suit seeking to recover damages from merchants. These suits seek to recover over and beyond what the card brand assessments might recover. These suits allege theories sounding in tort, contract, or both. Examples of claims can include negligence, negligence per se, various state unfair competition and consumer protection claims, and breach of contract (third-party beneficiary) claims.

For example, after the highly-publicized Target data breach, issuing banks brought suit against Target. The issuing banks alleged that Target was negligent in failing to provide sufficient security to prevent the hackers from accessing customer data and that its violation of Minnesota’s Plastic Security Card Act was negligence per se. The court certified the class of issuing banks. In another example, financial institutions brought suit against Wendy’s seeking to recover costs associated with customer reimbursements and those associated with operational expenses such as notifying customers, reissuing cards, closing accounts, monitoring and other measures to protect themselves. And most recently, Home Depot agreed to settle claims brought by a class of

12. Id. at *3
13. Id. at *12-14.
14. Id. at *25.
15. Id.
16. See e.g. In re Home Depot, Inc., 2016 U.S. Dist. LEXIS 65111, at *38 (N.D. GA May 17, 2016) (rejecting Home Depot’s argument that the claims were not ripe because the card brand recovery process was ongoing).
18. Id. at 487.
19. Id. at 490;
financial institutions for $25 million.\footnote{Allison Grande, Home Depot Deal May Spur Banks To Sue Data Breach Targets, LAW360 (March 14, 2017, 11:45 PM EDT), https://www.law360.com/consumerprotection/articles/901297/home-depot-deal-may-spur-banks-to-sue-data-breach-targets.} Given this trend, merchants not only have to be aware of their contractual liability, but also the threat of class action litigation from other affected financial institutions.

IV. CONCLUSION

Merchants must be particularly attentive to the risks associated with a data breach and cognizant of the potential liability that can arise as a result of such a breach—especially if they do not maintain PCI compliance. Merchants should recognize the scope of their responsibilities under their agreements with their acquiring banks, and that the PCI process does not shield merchants from suits by issuing banks for costs incurred by the fraud.
GOVERNMENT ENFORCEMENT WHEN PRIVATE DATE INFORMATION IS BREACHED: GUIDANCE AND BEST PRACTICES

Jacob D. Mahle*, Nathan Colvin**, and Emily St. Cyr***

I. INTRODUCTION

A data breach implicates many federal and state regulators. These regulators have the power to penalize entities for failure to implement privacy measures to protect consumer information, and for the violation of the applicable privacy laws.

Among the most important regulators that a data privacy practitioner must consider are:

- U.S. Department of Health and Human Services (HHS);
- Office for Civil Rights (OCR);
- U.S. Federal Trade Commission (FTC);
- U.S. Securities and Exchange Commission (SEC); and
- State Regulators (such as states attorneys general, departments of health, and departments of consumer affairs).

The landscape of privacy law is constantly evolving. There are many considerations and best practices that business should keep in mind both in dealing with these regulators, and in working to prevent data breaches from happening in the first place.

II. OFFICE FOR CIVIL RIGHTS: BREACHES INVOLVING PERSONAL HEALTH INFORMATION

Companies should be particularly concerned about breaches involving personal health information. Breaches involving health information are generally regulated through the Office of Civil Rights of the U.S. Department of Health & Human Services (“OCR”). The OCR does so through the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191, which was enacted to improve the efficiency and effectiveness of the health care

---

* Mr. Mahle is a partner at Vorys, Sater, Seymour and Pease, LLP and a member of the litigation section.
** Mr. Colvin is an associate at Vorys, Sater, Seymour and Pease, LLP and a member of the litigation section.
*** Ms. St. Cyr is an associate at Vorys, Sater, Seymour and Pease, LLP and a member of the litigation section.
There are three primary HIPPA Rules applicable to cybersecurity law: (1) the Privacy Rule, which sets forth national standards for the protection of individually identifiable health information for covered entities; (2) the Security Rule, which sets forth national standards for protecting the confidentiality, integrity, and availability of electronic protected health information; and (3) the Enforcement Rule, which provides standards for the enforcement of all the Administrative Simplification Rules. Covered entities include health plans, health care providers, and health care clearinghouses. The OCR can also regulate business associates, which are defined as a person or organization, other than a covered entity, “that performs certain functions or activities on behalf of, or provides certain services to, a covered entity that involve the use or disclosure of individually identifiable health information.” This broad definition of business associates potentially implicates a wide variety of entities that provide service to health care providers.

The OCR enforces HIPAA Rules in several ways, including:

- Investigating complaints of HIPAA violations filed with it;
- Conducting compliance assessments and audits of covered entities and business associates; and
- Educating covered entities and business associates on the requirements found in the HIPAA Privacy Rule and Security Rule.

Failure to comply with HIPAA Rules could result in corrective action by the OCR, including the imposition of millions of dollars of fines. In fact, to date, the OCR has settled 41 data breach cases, resulting in a total dollar amount of $48,679,700.00 in fines.
Covered entities are required to develop and distribute notices that provide individuals with a clear explanation of their privacy rights. The OCR and HHS have developed and published model Notices of Privacy Practices (NPP) that covered entities should use as a guide to ensure compliance with the HIPPA Rules. These model NPPs are published online at HHS.gov.

III. FEDERAL TRADE COMMISSION: FIVE PRINCIPLES OF DATA SECURITY PLANS

The Federal Trade Commission enforces data privacy laws through statutes such as the Gramm-Leach-Bliley Act, the Fair Credit Reporting Act, and the Federal Trade Commission Act. It has been doing so since the 1970s when it began enforcing the Fair Credit Reporting Act. The FTC works for the benefit of consumers to prevent fraudulent, deceptive, and unfair practices. At the same time, however, it also provides information to businesses to help them comply with the law.

According to the FTC, a “sound” data security plan is based on five principles, which are:

1) **Take Stock** of what personal information a business has in its files and on its computers;
2) **Scale Down,** to keep only what it needs for business;
3) **Lock It,** to protect the information a business does keep;
4) **Pitch It,** to properly dispose of what it no longer needs; and
5) **Plan Ahead,** to create a plan to respond to security incidents.

These principles can—and should—be adapted based on the size and nature of a business as well as the type of information collected from consumers.

A. In the Matter of LabMD, Inc.

The FTC is, of course, also able to investigate data privacy issues, and to impose penalties on companies that fail to comply with applicable data breach

---

9. *Id.*
10. *Id.*
14. *Id.*
15. *Id.*
laws. As of late, this includes the FTC bringing enforcement actions against companies that allegedly violate consumer privacy rights or mislead consumers.16

One of the most important recent examples of FTC enforcement is *In the Matter of LabMD, Inc.* Dkt No. 9357. On August 29, 2013, the FTC filed a complaint against LabMD alleging that it failed to protect consumers’ data, including private health information.17 Unlike a typical FTC enforcement action, LabMD did not settle the complaint with the FTC, but instead opted to litigate the case. In November 2015 the Administrative Law Judge (ALJ) assigned to the action dismissed the case, finding that the FTC had not met its burden of proof in showing an “unfairness” action.18

However, on July 29, 2016, the FTC reversed the ALJ’s decision. It found that LabMD’s security practices were unreasonable, “lacking even basic precautions to protect the sensitive consumer information maintained on its computer system.”19 LabMD’s unreasonable practices included failure to use an intrusion detection system or file integrity monitoring; neglecting to monitor traffic coming across its firewalls; providing essentially no data security training to its employees; and never deleting any of the consumer data it had collected.20

As a result of the enforcement action, LabMD was ordered to, among other things, maintain a comprehensive security program documented in writing; obtain periodic assessments and reports from an independent third party, which it must provide to the Director of Enforcement for the Bureau of Consumer Protection of the FTC; provide notice to individuals affected by the data breach; and make its compliance documents available to the FTC.21

The LabMD decision is currently on appeal to the United States District Court for the Eleventh Circuit, and a stay of the FTC Final Order was granted in November 2016.22 This is the first data security action litigated before the FTC and appealed to a United States Court of Appeals—and the decision will thus have an important impact on FTC investigations and regulations going forward, including the extent to which the FTC may regulate and bring enforcement actions in this space. Nevertheless, LabMD highlights the high costs an entity can face when going forward in a legal enforcement action with the FTC, as opposed to working with the FTC to obtain an early settlement, and demonstrates the importance of implementing and executing data breach policies.

17. *In the Matter of LabMD, Inc.* Dkt No. 9357, Complaint.
20. *Id.*
21. *In the Matter of LabMD, Inc.* Dkt No. 9357, Final Order.
22. LabMD, Inc. v. Fed. Trade Comms’n, 776 F.3d 1275 (11th Cir. 2015) (granting Time Sensitive Motion to Stay Enforcement of the Commissioner’s Final Order Pending Appeal and for a Temporary Stay While the Court Considers the Motion filed by Petitioner LabMD, Inc.).
IV. SECURITIES AND EXCHANGE COMMISSION
GUIDANCE AND REGULATION

The Securities and Exchange Commission also has the authority to penalize companies for failure to comply with cybersecurity laws and best practices. In April 2015, the SEC Division of Investment Management issued an Investment Management Guidance Update on cybersecurity. It recommends that, among other practices, businesses:

- Conduct periodic assessments to identify cybersecurity threats and areas of vulnerability in order to prioritize and mitigate risk;
- Create a strategy designed to prevent, detect and respond to cybersecurity threats; and
- Adopt written policies and procedures to implement the strategy.

A. In the Matter of Morgan Stanley Smith Barney LLC

Recently, the SEC initiated an investigation of Morgan Stanley Smith Barney LLC (Morgan Stanley) related to its private customer data, which was hacked and offered for sale online. On June 8, 2016, an order memorialized the SEC’s settlement with Morgan Stanley whereby Morgan Stanley agreed to pay a civil money penalty in the amount of $1 million. The investigation began, and the penalties were issued, for Morgan Stanley’s “failure to adopt written policies and procedures reasonably designed to protect customer records and information.”

While the SEC has labeled its April 2015 publication as “guidance,” it is clear from the Morgan Stanley settlement that companies would be wise to implement, and enforce, the SEC’s suggestions.

V. PRACTICAL CONSIDERATIONS

When responding to cybersecurity regulators—or any government entity, generally—there are practical considerations to keep in mind.

A. Adopting Written Data Breach Policies and Procedures

Almost all of the guidance set forth by the OCR, SEC, FTC and other data breach regulators dictates that businesses should plan ahead and develop written data breach policies. These policies can help businesses to avoid data breaches

24. Id.
27. Id.
altogether, and, should a breach occur, to mitigate any potential damages or penalties.

B. Dealing with Regulators

The stakes are high during an investigation, and how a business interacts with a regulator—both at the outset, and throughout the investigation—can make all the difference in the outcome of an investigation. When dealing with regulators, companies should disagree with negative findings, but not be disagreeable. It is important to establish a rapport with the regulator and to maintain that rapport throughout the investigation.

Further, companies should understand the different approaches, concerns, goals, and available penalties and regulation tools of the different regulators. There are a number of entities that can enforce cybersecurity rules and the practices and procedures of those entities are different, along with their goals. Overall, a business should work to understand the regulator, and create the best relationship possible with the investigator. Doing so will positively shape the view of the company’s conduct and benefit the company in coming to a resolution of the matter.

C. Internal Investigations and Protecting Them

An initial matter to consider during a data breach investigation is the ability of an entity to conduct internal investigations, and (critically) to protect the confidentiality of those investigations. In the rush to figure out what has happened in a data breach, the investigation, and its potential use against a company later by regulators and/or private litigants, needs to be kept at the forefront. This includes the extent and possibility of protecting a company’s internal investigation from disclosure through the attorney-client privilege and/or the work-product privilege. The key to maximizing any potential privilege is the involvement of attorneys, whether inside or outside the company, from the earliest stages of the investigation.

A company may also face decisions about disclosure. Many questions about disclosure are covered by applicable statutes and regulations, but gray areas remain. A company may have leeway with when to disclose, what to disclose, and who will receive the disclosure. Policies and procedures for internal investigations, protecting those investigations, and internal practices for disclosures should all be written into a company’s data breach plan.

D. Weighing the Business Decision

Ultimately, dealing with an enforcement action is a business decision. A company may face penalties, fines, and more, but it must also consider the effect of its response to the enforcement action on both its financial stability and reputation—which may be far more important than any regulatory action.
Winning the battle with a regulator over data breach questions is irrelevant if the company loses the war through damages caused to its brand by the breach.
CONSUMER CLASS ACTIONS ARISING FROM DATA BREACHES PRESENT A BATTLEGROUND FOR STANDING TO BRING SUIT

Eric W. Richardson*, Nathan L. Colvin**, and Timothy C. Dougherty***

I. INTRODUCTION

Announcements of data breaches quickly turn the gears of the court system, as class action attorneys waste little time in acting upon the potential large-scale liability from such breaches. When Target announced in December 2013 that it had suffered a data breach that potentially exposed information for forty million customers, fifteen class action lawsuits were filed against the company within a week.1 This comes as no surprise when the damages from a class action suit can stretch over the hundred-million-dollar mark and the average attorney fees for data breach litigation is more than one million dollars.2 Of course, class action plaintiffs’ counsel want to establish position to control major litigation that is a prime candidate for expansion into even larger multidistrict litigation. But in many cases, plaintiffs’ counsel may be acting too quickly by filing before identifying a putative class representative with an injury sufficient to establish standing and invoke the court’s jurisdiction.

II. STANDING REQUIREMENTS RESTRICT LAWSUITS TO CLAIMS ALLEGING ACTUAL INJURY

Consumer class actions arising out of data breaches arise under numerous theories of liability, ranging from negligence, breach of fiduciary duty, and breach of implied contract to invasion of privacy and state and federal statutory violations such as the Fair Credit Reporting Act, 15 U.S.C. § 1281 et seq. However, regardless of the claims, all plaintiffs must establish standing to get into federal court. To establish standing to maintain a lawsuit in federal court

---

* Mr. Richardson is a litigation partner at Vorys, Sater, Seymour and Pease LLP, where he has represented clients in class action litigation involving data breaches. Mr. Richardson is also an adjunct faculty member at the Salmon P. Chase College of Law, where he teaches Information Privacy Law and Intellectual Property Law.

** Mr. Colvin is a litigation associate at Vorys, Sater, Seymour and Pease LLP, where he has represented clients in class action data breach litigation.

*** Mr. Dougherty is a litigation associate at Vorys, Sater, Seymour and Pease LLP.


under Article III of the United States Constitution, an injury must be “concrete, particularized, and actual or imminent; fairly traceable to the challenged action; and redressable by a favorable ruling.”

Thus, a plaintiff must have suffered an actual or imminent injury that the litigation can recompense. These requirements are established to ensure the judicial branch does not usurp the policymaking roles of the political branches. For harm to qualify as imminent, the “threatened injury must be certainly impending.” Harm that is merely possible or speculative is not sufficient to invoke the jurisdiction of the federal courts, and state courts largely follow these same rules. Data breach cases have frequently tested this requirement.

III. FACTUAL HURDLES TO CLEAR TO SHOW STANDING IN DATA BREACH CLAIMS

Unless an action is brought pursuant to a statute that specifies the kind of injury sufficient to give rise to a suit, for plaintiffs to show actual injury in data breach cases, they typically will need to clear two important hurdles. First, plaintiffs must show that their data was actually accessed in a meaningful way by hackers. In other words, plaintiffs must show that their data was personally identifiable information and that it was actually exfiltrated by the hackers. Did the hackers just hack into the system or did they actually exfiltrate information? Was the data personal information of such a nature that a group of plaintiffs could be harmed if that information was actually used? Was the data encrypted to a degree that it would be useless to hackers regardless of the underlying data contents? Although someone may not want a hacker to have one’s name, showing harm from that information alone is more difficult than showing harm from the theft of one’s name and a Social Security number or a credit card.

4. Id. at 1146.
5. Id. at 1147 (emphasis in original).
6. See, e.g., Cleveland v. Shaker Hts., 507 N.E.2d 323, 325 (Ohio 1987) (“[T]he question of standing depends on whether the party has alleged. . . a personal stake in the outcome of the controversy.”) (internal quotation marks omitted); see also Kincaid v. Erie Ins. Co., 944 N.E.2d 207, 210 (Ohio 2010) (finding no justiciability where plaintiff had not yet suffered loss).
7. Most data breach class actions allege common law tort or contract claims. However, in some instances, class action plaintiffs have brought statutory claims based on statutes that specify a lower threshold of injury that is sufficient to bring suit. See, e.g., Matera v. Google Inc., No. 15-cv-04062, 2016 U.S. Dist. LEXIS 130778, at *41 (N.D. Cal. Sept. 23, 2016) (holding that invasion of privacy is injury sufficient to grant standing pursuant to the Wiretap Act 18 U.S.C. § 2511(a)(1) and the California Invasion of Privacy Act, Cal. Penal Code § 631).
8. See In re Sci. Applications Int’l Corp. (SAIC) Backup Tape Data Theft Litig., 45 F. Supp. 3d 14, 20 (D.D.C. 2014) (noting that because the tapes were lost rather than stolen and were encrypted reduced the likelihood the personal information would be accessed); Reilly v. Ceridian Corp., 664 F.3d 38, 42 (3d Cir. 2011) (concluding that despite a breach, there was no showing that the hacker actually read, copied or understood the personal information).
9. See SAIC, 45 F. Supp. 3d at 20; Reilly, 664 F.3d at 42.
number. Likewise, even the most sensitive personal information may not give rise to harm if there is little reason to think the thief will be able to do anything with the information. If the plaintiffs’ data was encrypted, or was never exfiltrated by the hacker, then the data may not have been accessed in a meaningful way by hackers.

Second, assuming that the plaintiffs can show that their stolen personal information was accessed in a meaningful way, the plaintiffs must then demonstrate that their data was actually misused by hackers or is in imminent danger of being misused. Because class action suits are frequently filed before the named plaintiffs have any evidence of actual misuse of their data, both circuit and district courts around the country have struggled with how to apply traditional standing rules to a threat of potential misuse of personal data.

IV. ACTUAL MISUSE OF DATA SATISFIES REQUISITE HARM

As an initial matter, courts uniformly have found that actual misuse of a plaintiff’s personally identifiable information is sufficient to establish standing. Where plaintiffs can show that the theft of their information has led to identity theft, new lines of credit being taken in the plaintiffs’ names, injury to their credit rating and the like, courts have found that actual harm has been incurred and, thus, the requirements of standing have been satisfied. For example, in Lambert v. Hartman, the Sixth Circuit held that a plaintiff had adequately established the requirements of standing where the plaintiff demonstrated that the hacker’s theft and misuse of her personal information had injured her credit rating. In Resnick v. AvMed, Inc., the Eleventh Circuit similarly found that the

---

10. C.f. SAIC, 45 F. Supp. 3d at 20 (intimating that even a name and Social Security number may not be as harmful as financial data such as credit card information).
11. Id.; Reilly, 664 F.3d at 42.
12. See SAIC, 45 F. Supp. 3d at 25, 28, 31 (requiring actual misuse connected to alleged harm); Krottner v. Starbucks Corp., 628 F.3d 1139, 1141-43 (9th Cir. 2010) (finding credible threat of immediate harm when a laptop with personally identifiable information was stolen).
14. See, e.g., Lambert v. Hartman, 517 F.3d 433, 437 (6th Cir. 2008) (holding that the plaintiff had established standing where plaintiff “alleged that her identity was stolen and that her financial security and credit rating suffered as a result.”); Resnick v. AvMed, Inc., 693 F.3d 1317, 1323, 1329-30 (11th Cir. 2012) (“Plaintiffs allege that they have become victims of identity theft and have suffered monetary damages as a result. This constitutes injury in fact under the law.”).
15. Lambert, 517 F.3d at 437; Resnick, 693 F.3d at 1323.
16. Lambert, 517 F.3d at 437 (holding that the plaintiff had established standing where plaintiff “alleged that her identity was stolen and that her financial security and credit rating suffered as a result.”).
plaintiff had established standing where the hacker’s theft of unsecured laptops had led to unauthorized lines of credit being opened in the plaintiffs’ names.17

V. COURTS STRUGGLE WITH DRAWING THE LINE FOR STANDING IN DATA BREACHES

While courts had no trouble finding standing where there was an allegation of actual misuse of personally identifiable information, the first courts to deal with class actions that lacked such allegations split on the question of standing.

The majority of courts first addressing this question found standing where plaintiffs had merely alleged an increased risk of harm. For example, in Pisciotta v. Old National Bancorp, the Seventh Circuit held that standing was established in a data breach where the plaintiffs spent resources on credit monitoring and suffered an “increase[ed] risk of future harm.”18 Further, in Krottner v. Starbucks Corp., the Ninth Circuit held that the risk of harm posed by the theft of a laptop with unencrypted names, addresses, and Social Security numbers posed a “credible threat of harm” that was “real and immediate, not conjectural or hypothetical,” even though no actual misuse had occurred by the time of the lawsuit.19 Indeed, some courts even held that “the fear or anxiety of future harm” – even in the absence of any actual harm – is a sufficiently cognizable injury to establish standing.20 Other courts analogized data breaches to toxic tort cases, where no actual harm has been suffered yet, but the court presumes that an injury will occur in the future due to the plaintiff’s “exposure.”21

Nonetheless, not all courts have allowed a plaintiff to proceed merely on a showing of an increased risk of harm. In fact, a minority of courts has refused to find standing without an allegation of actual harm or actual misuse of a plaintiff’s personally identifiable information. In the seminal minority position case, Reilly v. Ceridian Corp., the Third Circuit Court of Appeals considered a data breach where a hacker had infiltrated a company’s security, but the plaintiff could not show that the hacker had actually read, copied or understood the personal information, nor that the hacker intended or was capable of criminal misuse.22

17. Resnick, 693 F.3d at 1323, 1329-30 (“Plaintiffs allege that they have become victims of identity theft and have suffered monetary damages as a result. This constitutes injury in fact under the law.”); Curry v. AvMed, Inc., No. 10-cv-24513, 2014 U.S. Dist. LEXIS 48485, at *2-3 (S.D. Fla. Feb. 28, 2014) (preliminary certification of two classes the theft of whose personal identifying information gave the class standing).
18. Pisciotta v. Old Nat’l Bancorp, 499 F.3d 629, 634 (7th Cir. 2007) (standing satisfied by “increased risk of future harm”).
19. Krottner v. Starbucks Corp., 628 F.3d 1139, 1141-43 (9th Cir. 2010) (finding credible threat of immediate harm when a laptop with personally identifiable information was stolen).
Under those circumstances, the Third Circuit concluded that the plaintiffs failed to establish standing because the potential harm was “neither imminent nor certainly impending.”23 and it rejected the proposition that increased risk alone is sufficient to establish standing.24 Further, even though the plaintiffs had paid for credit monitoring services in the wake of the data breach, the court held that such costs were voluntarily undertaken in the absence of an imminent harm and, thus, plaintiffs’ choice to pay these costs could not establish actual harm to the plaintiffs.25

VI. CLAPPER REINFORCES STANDING BAR AGAINST CONJECTURAL HARM, ALBEIT IN A DIFFERENT CONTEXT

The United States Supreme Court has not yet addressed the question of standing in a data breach context. But in 2013, in Clapper v. Amnesty International, the Supreme Court issued a critical Article III standing decision dealing with the absence of a showing of actual harm, which has greatly impacted the way lower courts have addressed standing in data breach class actions.26

Specifically, the Clapper Court considered a challenge by Amnesty International and others as to the constitutionality of the Foreign Intelligence Surveillance Act, through which the Attorney General and the Director of National Intelligence were authorized to obtain approval from the Foreign Intelligence Surveillance Court to conduct surveillance on individuals who are not “United States persons” and who are reasonably believed to be located outside of the United States.27 Notably, such surveillance could be authorized without a showing of probable cause to believe that the target of the surveillance was, in fact, an agent of a foreign power.28

In that case, the plaintiffs alleged that there was an objectively reasonable likelihood that the communications of Amnesty International’s employees—who are United States residents who regularly communicate during the course of their employment with the potential targets of the statute—would be intercepted pursuant to the statute.29 The plaintiffs also alleged that the risk of surveillance under the statute was so substantial that they had to take costly measures to secure their communications.30

Notwithstanding the expressed concerns, the Supreme Court rejected the plaintiffs’ arguments and held that they had failed to demonstrate actual or

23. Id. at 42-43.
24. Id. at 43.
27. Id. at 1140.
28. Id. at 1144.
29. Id. at 1146.
30. Id.
imminent harm sufficient to establish standing. The Supreme Court held that the plaintiffs’ theory of standing required speculation that Government actors would actually target plaintiffs’ communications; that they would do so via the statutory authorization instead of a traditional warrant; and that the Government would successfully acquire the communications. The Court also rejected the claim that plaintiffs had already suffered harm by taking security precautions fairly traceable to the statute because precautions taken without an imminent threat of harm are not fairly traceable. In short, the Supreme Court held that a plaintiff’s “subjective fear of surveillance does not give rise to standing.”

VII. INCONSISTENT ATTEMPTS BY COURTS TO APPLY 
CLAPPER
TO DATA BREACH CASES

In the aftermath of Clapper, district courts were initially “more emphatic in rejecting ‘increased risk’ as a theory of standing in data-breach cases.” Rather than a “credible threat” of harm, those courts required a more exacting factual basis before finding an imminent threat of injury.

For example, the District Court for the District of Columbia found no imminent threat of injury where a car theft resulted in the loss of backup tapes with names, Social Security numbers, dates of birth, and medical information (but not bank or credit card information), because those tapes required specific hardware and software to understand and use. Similarly, an online breach of personally identifiable information from eBay accounts (but not bank or credit information, nor Social Security numbers) did not demonstrate an imminent threat of injury because there had been no allegation of misuse (or attempted misuse) of the information. And earlier this year, the District Court of Minnesota found no standing where plaintiffs alleged a data breach involving malicious software installation to the portion of a network that processed credit card payments—even when one plaintiff faced a fraudulent charge on his credit card—because (i) none of the other sixteen plaintiffs faced similar actions and (ii) the lone plaintiff affected did not allege ultimate monetary loss because he immediately cancelled his credit card.

Matters were looking so bleak for class action plaintiffs that some enterprising attorneys began to allege that the plaintiffs were injured because

---

31. Clapper, 133 S. Ct. at 1155.
32. Id. at 1147-48.
33. Id. at 1151.
34. Id. at 1152-53.
36. Id. at 20, 30.
their personally identifiable information was less valuable on the black market as a result of a data breach. In the district court proceedings in *Galaria v. Nationwide Mutual Insurance Co.*, for example, plaintiffs alleged that there is a “cyber black market” in which they could sell personal information for profit and that the hacking deprived them of that value. Not surprisingly, the district court found that plaintiffs had not sufficiently alleged how they had been deprived of the value of their personal information by being deprived of the opportunity to sell that information on the black market.

Despite this initial trend towards more rigorous standing in the immediate aftermath of *Clapper*, the courts of appeals have begun to swing back to the pre-*Clapper* view of standing in data breach cases. In *Galaria*, for example, the Sixth Circuit reversed the district court and concluded the plaintiffs had standing, noting that there was a “sufficiently substantial risk of harm” and that it would be “unreasonable to expect Plaintiffs to wait for actual misuse” of their personally identifiable information before bringing suit. Continuing, the Sixth Circuit noted that, as a result of the hack, the plaintiffs’ information was possessed by criminals and, thus, that harm to the plaintiffs was likely to be imminent—reasoning that would appear to apply to virtually all hacking and other theft cases. (The Sixth Circuit did not address plaintiffs’ argument that, as a result of the hack, their personally identifiable information was less valuable and that the plaintiffs would be unable to sell their own information for as much as they might otherwise have.)

Similarly, courts in the Seventh and Ninth Circuits have concluded that *Clapper* did not disturb the pre-*Clapper* decisions in *Pisciotta* and *Krottner*. In *Remijas v. Neiman Marcus Group, LLC*, the Seventh Circuit distinguished *Clapper* by noting that, whereas there was no evidence that any plaintiffs were monitored by the Government in *Clapper*, the credit card information of the plaintiffs in the case at bar was known to be stolen and, further, around three percent of the accounts had been the target of fraudulent activity. Thus, the Seventh Circuit held that there was an “objectively reasonable likelihood” that the plaintiffs would suffer injury in the future and that such a prospect established standing, despite the Supreme Court’s seeming rejection of that standard under the *Clapper* facts. Similarly, in *Corona v. Sony Pictures Entertainment, Inc.*, the Central District of California found that *Krottner’s* “credible threat of real and immediate harm” standard survives *Clapper* despite differences in language. In *Corona*, the court found real and immediate risk of

---

40. *Id.* at 659-60.
42. *Id.* at *9-10.
harm where plaintiffs alleged that personal information was stolen and posted on a file-sharing website for identity thieves to access and where some plaintiffs had received threats of harm to its employees.45

VIII. THE NEXT HURDLE ON THE HORIZON: HARM SUFFICIENT TO STATE A CLAIM

The most recent trend of appeals courts distinguishing Clapper in data breach class actions could prove to be temporary, as courts turn their attention to whether the plaintiffs have pleaded actionable harm sufficient to state a claim for relief. Although this difference was noted by courts prior to Clapper, the hurdle was clearly demonstrated by a recent district court case that followed the Seventh Circuit’s post-Clapper standing decision. In In re Barnes & Noble Pin Pad Litigation (N.D. Ill. Oct. 3, 2016), the court found a “substantial risk” of harm to plaintiffs sufficient to satisfy standing where the plaintiffs were Barnes & Noble customers who made purchases during a period in which skimmers stole data from store pin pad terminals and were alleged to have used such data for unauthorized purchases.46 However, because no actual out-of-pocket loss was alleged, the court found that, although plaintiffs had standing to bring suit, they failed to allege damages sufficient to plead their causes of action, resulting in dismissal of their claims.47

IX. CONCLUSION

More courts will undoubtedly continue to struggle with applying the Supreme Court’s Clapper decision in the data breach context and to draw the line for the standing of class action plaintiffs. But even if the battleground ultimately moves from the issue of standing – as more courts adopt the lesser threshold recently articulated by the Sixth and Seventh Circuits – plaintiffs will likely be challenged if they cannot allege sufficient damages in support of their causes of action. And whether such hurdles begin to curtail consumer class actions has yet to be determined.

45. Id. at *5-6.
47. See, e.g., id. at *15-16, 24-25.
A "GOLDEN KEY" TO PANDORA’S BOX:  
THE SECURITY RISKS OF GOVERNMENT-MANDATED BACKDOORS TO ENCRYPTED COMMUNICATIONS

Alexa Wainscott

I. INTRODUCTION

In the wake of the gruesome terror attacks on Mumbai in 2008, Indian government officials quickly sought to amend the nation’s Information Technology Act to expand law enforcement’s ability to decrypt suspect communications. Fast forward seven years, and cybersecurity fears surrounding the use of encryption technology again dominated Indian media, but for entirely opposite reasons. The public reaction to heightened communication access for law enforcement shifted when the Indian Ministry of Communications and Information Technology introduced its draft of a new and controversial national encryption policy proposal, inciting widespread panic among technology consumers. Opponents of strict electronic and digital surveillance laws construed portions of the proposed plan as requiring users to store the unencrypted plain text versions of messages for up to ninety days, or potentially face penalties. Users of WhatsApp, Facebook, Viber, and other instant messaging and Voice Over Internet Protocol (VoIP) apps were ultimately relieved of their fears when the proposal was withdrawn by Telecom minister Ravi Shankar Prasad in September 2015.

Although the scope of discussion in this Note is limited to communications access issues in the United States, these issues are global in nature, as the current web of interconnected technology developers and users spans worldwide. This renders the policy position of the United States on encryption technology, and most recently, in response to the high-profile legal battle between Federal Bureau of Investigation (FBI) and Apple, Inc., even more critical on an international scale. The response of the United States in particularly prominent cases such as

---

3. Id.
4. Id.
6. Id.
this inevitably shapes the future of technology development and cybersecurity around the world.

National policies concerning cryptography have great influence upon technology developers and manufacturers, which include some of United States’ largest employers and most profitable corporations. If national regulations are inconsistent or become unduly burdensome, these corporations may cease to operate within the United States and relocate to other regions of the global market in which they already operate. Consequently, it is imperative to analyze the encryption policy positions of the United States within a global context to appreciate the full impact any policies might have on our nation’s future economic and technological landscape.

The practical future of data protection and cybersecurity necessitates embracing and improving modern encryption technology. However, increased reliance on cryptography in communications systems has created tension between technology manufacturers, communications service providers, and law enforcement as to the level of access law enforcement may have to encrypted messages and other forms of communication. Warrants are no longer sufficient to ensure law enforcement access to suspect communications because legal access is becoming significantly less of a barrier than physical access to the unencrypted versions of communications. Massachusetts District Attorney Dan Conley has been a particularly zealous advocate of exceptional access for law enforcement, i.e. unfettered government access to private communications, as an essential matter of public safety and security. Conley has been well-known for his advocacy for increased government access and surveillance:

“In America, we often say that none of us is above the law,” Conley said in his prepared remarks. “But when unaccountable corporate interests place crucial evidence beyond the legitimate reach of our courts, they are in fact granting those who rape, defraud, assault, and even kill a profound legal advantage over victims and society.”

Conley warned Congress of the horrors to ensue if the national government is unable to pierce the technological barrier between itself and target

---


8. Id.


10. Id.
communications stored by large technology corporations such as Apple, Google, and others.\textsuperscript{11}

This view certainly embodies one end of the encryption policy spectrum, a position shared by many law enforcement officials, including the FBI Director.\textsuperscript{12} It was this realm of policy concerns regarding communications access that led to the enactment of the Communications Assistance for Law Enforcement Act (CALEA) in 1994.\textsuperscript{13} CALEA, in a general sense, implemented a “mandate requiring service providers to provision their networks in a way that will enable law enforcement wiretapping capabilities.”\textsuperscript{14} Congress drafted and enacted this legislation, which established communications access requirements, with the traditional Public Switched Telephone Network (PTSN)\textsuperscript{15} (also referred to as the Plain Old Telephone Service) in mind. The mandate does not contemplate and is insufficient to address the rapidly expanding field of encryption technology.

As a result, law enforcement has faced three recent technological challenges that have demonstrated some of CALEA’s core contemporary weaknesses: (1) default encryption in communications systems, (2) end-to-end-encryption,\textsuperscript{16} and (3) telecommunications services that fall outside of the parameters of CALEA\textsuperscript{17} and thus are not covered by its mandate for surveillance-enabling features.\textsuperscript{18} For example, CALEA envisioned primarily traditional client-server schemes, where telecommunications carriers\textsuperscript{19} are those engaged in the transmission of electronic


\textsuperscript{12} See Pell \textit{supra} note 9.


\textsuperscript{14} See Pell \textit{supra} note 9 at 604-06.

\textsuperscript{15} The Federal Communications Commission (FCC) has predicted that PTSN will effectively become obsolete by 2018. See Steven M. Bellovin et al., \textit{Lawful Hacking: Using Existing Vulnerabilities for Wiretapping} on the Internet, 12 NW. J. Tech. & Intell. Prop. 1, 9 (2014).

\textsuperscript{16} Initially, communications service providers began encrypting user data with a key that was accessible to the provider. However, recently providers and applications, such as Apple’s iMessage, have shifted towards encryption methods using keys inaccessible to even the provider. That is, the unencrypted plain text versions of data are only available to the user on the individual’s device. See Pell \textit{supra} note 9 at 604.

\textsuperscript{17} The discussion of government inability to access communications, due to lack of authority over certain manufacturers and communications service providers, is commonly referred to as the “Going Dark Debate.” See generally Urs Gasser et al., \textit{Don’t Panic: Making Progress on the Going Dark Debate, The Berkman Center for Internet & Society at Harvard University} (Feb. 1, 2016), https://cyber.law.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf (presenting a clear overview of emerging encryption issues and responses to the Going Dark Debate).

\textsuperscript{18} See Pell \textit{supra} note 9.

\textsuperscript{19} CALEA defines a “telecommunications carrier” to mean “a person or entity engaged in the transmission or switching of wire or electronic communications as a common carrier for hire.” Pub. L. No. 103-414, § 102(8)(A).
or wire communications between themselves and users.20 However, the existence of alternate schemes, such as peer-to-peer networks,21 have inhibited the wiretapping and data collection activities of law enforcement. Proponents of government surveillance have advocated an extension of CALEA (colloquially, CALEA II)22 to cover all variations of communications systems, but opponents claim this raises numerous cybersecurity challenges.23

Regardless of one’s position on the policy spectrum of encryption and law enforcement accessibility, it can be mutually agreed that CALEA is no longer sufficient legislation, and we are living in a practical post-CALEA reality.24 The prevalence of new and rapidly developing encryption technology has graduated us from the traditional era of PSTN communications to new and uncertain ground. However, this cannot come entirely as a surprise, as the Federal Trade Commission (FTC) has actively advocated and enforced safeguards relating to encryption of sensitive user data; the FTC has routinely brought legal ramifications upon businesses that have failed to protect consumers in this regard.25 The FTC guidelines strongly encourage the use of encryption as a primary means of protecting data and preventing security breaches in corporate systems.26 As encryption expands and becomes stronger, and hackers get smarter, a practical conflict may develop; corporations must reconcile demands imposed by the agencies like the FBI, as well as other mandates regulating encryption technology and requiring implementation of “backdoors,” which leave devices and networks more susceptible to security issues.27

20. See Bellovin supra note 15 at 17.
21. While Skype was one of the most notable peer-to-peer schemes, it has made certain changes in its architecture. See Zack Whittaker, Skype Ditched Peer-to-Peer Supernodes for Scalability, not Surveillance, ZDNET.COM (Jun. 24, 2013 16:02 GMT), http://www.zdnet.com/article/skype-ditched-peer-to-peer-supernodes-for-scalability-not-surveillance/.
22. See Bellovin supra note 15 at 16; see generally Christa M. Hibbard, Note, Wiretapping the Internet: The Expansion of the Communications Assistance to Law Enforcement Act to Extend Government Surveillance, 64 FED. COMM. L.J. 371 (2012) (noting that “CALEA would likely be amended to be written in ‘technologically neutral’ terms to prevent its requirements from becoming obsolete” as technology progresses).
23. See Bellovin supra note 15 at 16. Three prominent cybersecurity concerns are: (1) it impedes technological innovation because it restricts application developers from creating certain models, (2) the extension would impose a financial burden on software developers, and (3) law enforcement access keys could create security holes that leave devices and our technological infrastructure itself more vulnerable to cybersecurity threats, such as computer crime and cyberespionage.
24. See generally Pell supra note 9 (noting that CALEA’s force has been gradually weakened by increased IP-based communications, not subject to the legislation’s requirements, and more recently, by increased default encryption in smartphones).
26. See Pell supra note 9 at 613.
27. See Pell supra note 9 at 609.
it increasingly difficult for all sorts of corporations, from cellphone developers to hospitals, to freely satisfy their ethical burdens in the way of user privacy, and they may require developers to sacrifice overall system functionality and reliability.

Two arms of the government are currently at odds with one another on the encryption policy spectrum; they are sending dangerously mixed messages to our communications service providers and app developers, on whom we rely heavily, and who we desperately need to remain competitive in a global economy.28 There currently exists a policy paradox, of sorts, regarding the matter. Consequently, our most technologically innovative corporations are left without sound guidance as to any practical cryptography policy and encumbered by the possibility of future federal mandates or demands, such as those Apple faced earlier this year. On the one hand, the FTC and our justice system impose high penalties on corporations who leave user or customer data susceptible to security breaches. On the other hand, requests like those made of Apple by the FBI and proposals to impose strict encryption access requirements discourage corporations from investing money in developing the securest encryption available.

It is necessary to determine what place the United States will assume on the spectrum of responses to encryption technology and what cybersecurity policies it genuinely wants to promulgate. Most critically, it is urgent to address the potential dangers of allowing federal mandates to become so burdensome on our most technologically advanced corporations that we discourage future corporations from incorporating and operating in the United States. The current state of conflicting guidance regarding encryption limitations and requirements is not a particularly attractive atmosphere for emerging technology enterprises.

II. BACKGROUND

The debate surrounding the emerging legal issues brought about by enhanced encryption technology is an expansive one. It encompasses discussion of privacy issues stemming from increased government access to communications, security issues raised by inhibited law enforcement ability to execute wiretap and other warrants, and additional security issues raised by technology developers on the other end of the spectrum. Attempting to strike a balance between the competing economic and policy concerns has proven to be a difficult task, and as the Indian Ministry of Communications and Information Technology observed in 2015, legislation limiting the use of encryption to protect user-data is not always well-

28. See generally Pell supra note 9 (noting that there are competing security interests at issue within our government, as it encourages increased cybersecurity measures and penalizes breaches for consumer security, but it must balance this interest with law enforcement’s duty to promote public safety).
received by consumers. A complete discussion of the legal and cybersecurity implications of cryptography must begin with a review of some previous attempts to address communications access through legislation, the ways in which communications technology has progressed in recent years, and the central issues surrounding the concept of “going dark.”

A. A Brief Review of CALEA and Related Legislation

CALEA was born during the rise of the Integrated Services Digital Network (ISDN) and mobile cellular telecommunications, which occurred during the early 1990s. Such increased ISDN use presented a difficulty for law enforcement because it was not possible to wiretap and intercept those communications using conventional means. In response, law enforcement sought to enact policies which would require telecommunications providers to facilitate law enforcement access to suspect communications. In the face of ardent opposition from service providers and civil liberties organizations, CALEA came into existence, but it was limited in scope such that only a specific subset of communications would be subject to the requirements in the Act.

Former Director of the FBI, Louis Freeh, addressed the limited scope of CALEA, comprising “phone-to-phone conversations which travel over a telecommunications network,” in 1994 during his Congressional testimony:

From what I understand, and again, I am probably the worst person in this room to answer the question, communications between private computers, PC-PC communications, not utilizing a telecommunications common net, would be one vast arena, the Internet system, many of the private communications systems which are evolving. Those we are not going to be on by the design of this legislation.

CALEA was expressly limited to interception of telephone communications and call-identifying information. Like all legislation, CALEA neither was


31. See Bellovin supra note 15 at 7.

32. Id.

33. Id.

34. Id. at 5.


36. See Bellovin supra note 15 at 10.

37. See US Telecom Ass’n vs. FCC, 227 F.3d 450, 454 (D.C. Cir. 2000) (“The Act defines ‘call-identifying information’ as ‘dialing or signaling information that identifies the origin,
created nor existed in a legal vacuum; it regularly called upon related legislation
to ensure law enforcement access to telecommunications. CALEA only
authorized interception of calls and call-identifying data after issuance of a
warrant pursuant to Title III\(^{38}\) of the Omnibus Crime Control and Safe Streets Act
of 1968.\(^{39}\) CALEA has also been invoked in conjunction with the Pen Register
Statute\(^{40}\) and the Stored Communications Act\(^{41}\) in order to compel disclosure of
prospective location data from cellular telephone service providers.\(^{42}\) In a
memorandum opinion issued by the United States District Court for the Southern
District of New York, the court found that the Pen Register Statute provided for
the actual installation of devices that would reveal users’ telephone numbers and
the prospective cell site location data for the beginning and end of call periods.\(^{43}\)
However, the court found that, in order to compel disclosure of the cell site data,
CALEA required supplemental statutory authority, and it ultimately called upon
the Stored Communications Act, determining that the combined language of the
statutes satisfied the disclosure requirements.\(^{44}\)

CALEA is perhaps too limited in scope to be effective alone, or to have great
staying power as technology progresses, diverse communications services
develop, and the prevalence of cryptography expands. Congress did not intend
CALEA to expand law enforcement access, but rather to maintain the status quo,
and to simply ensure that law enforcement agencies would not be technologically
locked out from communications that were legally accessible pursuant to a court-
issued warrant.\(^{45}\) The drafters of CALEA did not comprehensively account for
potential future developments in the rapidly-growing and ever-changing field of
information and communications technology, as evidenced by its limited scope.
This unfortunate lack of technological foresight has subsequently led to much of
the legislation’s waning effectiveness in recent years, as well as the increasingly
uncertain state of statutory authority relating to encryption use and regulation in
the storing and accessing of communications.

---

197 (1968). Text of Title III of the Act is available at https://it.ojp.gov/PrivacyLiberty/
authorities/statutes/1284.
42. *In re United States for Order for Prospective Cell Site Location Info.*, 460 F. Supp. 2d 448
(S.D.N.Y. 2006).
43. *Id.*
44. *Id.*
45. *See US Telecom Ass’n*, 227 F.3d at 454.
B. Technology Overview

At least a cursory understanding of the ways in which our technological landscape has changed is essential to the furtherance of meaningful discourse on the subject for encryption policies and legal requirements for providers. As Valerie Caproni, General Counsel of the FBI, noted in her Congressional testimony, there has been great change in our communication methodology, presenting unique challenges for law enforcement:

One result of this change is a transformation of communications services from a straightforward relationship between a customer and a single CALEA-covered provider (e.g. customer to telephone company) to a complex environment in which a customer may use several access methods to maintain simultaneous interactions with multiple providers, some of whom may be based overseas or otherwise outside the scope of CALEA.46

CALEA envisioned a world substantially like the PTSN telephony of the 1950s to the 1980s, with relatively few providers, whom the Act could bring within its statutory authority with relative ease.47 However, it is painfully clear that we are quickly distancing ourselves from traditional PTSN models, and those communications services that have recently emerged could not be more different in their operations, and consequently, legal implications.

1. Traditional PTSN Architecture

The PTSN refers to the digital switches,48 lines, and connections that have provided large-scale telephone service to the public since its inception as a manual mechanical switchboard in 1878.49 A review of more recent technological developments follows in the next subsection. For ease of understanding, a very basic diagram of a typical PTSN topography is depicted below:

46. See Bellovin supra note 15 at 1.
47. Id. at 6.
48. See generally The International Engineering Consortium, Signaling System 7 (SS7), ILLUMINET, https://www.cs.rutgers.edu/~rmartin/teaching/fall04/cs552/readings/ss7.pdf (last visited Feb. 27, 2017) (stating that PTSN modernly uses Signaling System No. 7 (SS7) to provide control signaling for the network; comprehensive discussion of the intricacies of SS7 is outside of the scope of this Note, but an interested reader may refer to the above article).
The actual topography of the PTSN infrastructure depends on its geographical location, as competitive markets are comprised of numerous interconnected service providers, but monopolized markets may have a single service provider operating the lines and switches. However, the general architecture of the PTSN is relatively static, with one primary model from which some networks deviate. PTSN integrates three basic types of nodes, and two basic methodologies for connecting switching nodes. End-Office (EO) nodes, or local exchanges, allow the user to access the network and exist as the basis of the architecture. Tandem nodes connect EOs together, organize traffic, and provide access to another hierarchical level of the network. Transit nodes provide access to yet another hierarchical level and are primarily used for connecting long-distance activity.

To connect the switching nodes, PTSN uses a combination of two patterns. The first involves direct connections between each communicating line. While this pattern is effective because it limits traffic build-ups by only connecting those lines that are in communication, it can become ineffective if there are many lines in the network. The second pattern is hierarchical and a bit more complex, “in which nodes are aggregated as the hierarchy traverses from the subscriber access points to the top of the tree.” The exact combination and interaction of these patterns to form the PTSN in any region is determined by a variety of economic and geographic factors.

50. Id.
51. Id.
52. Id.
53. Id.
54. Id.
55. See Dryburgh & Hewett supra note 49.
56. Id.
57. Id.
58. Id.
59. Id.
60. Id.
61. See Dryburgh & Hewett supra note 49.
In recent years, the internet, certain Voice over Internet Protocol (VoIP)\textsuperscript{62} technologies, and other communications services networks have altered the functionality of the PTSN. However, many VoIP systems still communicate with the PTSN, in a variety of relationships that only serve to complicate law enforcement interests.\textsuperscript{63} Albeit the fact that the PTSN is almost entirely digital in nature today to accommodate mobile phones, it is still significantly less functionally relevant today than it was at its inception.

2. Recent Developments in Communications Technology

Emerging Internet Protocol (IP) and VoIP technologies have presented a dilemma for law enforcement in executing wiretap warrants and accessing suspect communications.\textsuperscript{64} IP technology differs from the traditional PTSN architecture in several ways. Many communications providers have abandoned traditional PTSN architecture in favor of the IP model, which involves the exchange of IP data packets over the internet, digital circuits, and even in some instances still analog circuits.\textsuperscript{65} VoIP communication platforms have become increasingly popular among technology consumers, namely such high-profile platforms as Skype’s video chat, Apple’s FaceTime, and WhatsApp’s calling feature, among others. VoIP refers to technology that translates users’ voices into digital signals that can be transmitted using a broadband internet connection, as opposed to a traditional PTSN-style digital or analog telephone line, to provide users with calling and video chat features.\textsuperscript{66}

While some VoIP communications providers only allow users to interact with corresponding VoIP providers (such as FaceTime, which requires connection to another Apple device), others allow users to connect with regular PTSN telephone numbers, or to traditional telephones via a VoIP adapter.\textsuperscript{67} VoIP calling can be preferable to traditional telephone service in many aspects, such as the fact that service is available wherever an internet connection is provided, whether or not cellular service reaches the location.\textsuperscript{68} Although the FCC technically requires these VoIP communications service providers to comply with the regulations in CALEA, the practical application of such regulations to VoIP providers is highly nuanced and by no means a matter of black-letter law.

IP and VoIP technology hinders law enforcement access to communications in a number of ways, for example: (1) the VoIP provider may be located

\textsuperscript{62} Voice Over Internet Protocol, discussed infra Section II(B)(3).
\textsuperscript{63} Dryburgh & Hewett supra note 49.
\textsuperscript{64} See Bellovin supra note 15 at 9.
\textsuperscript{67} Id.
\textsuperscript{68} Id.
overseas\(^69\) (there is no requirement regarding the provider’s proximity to the subscriber), the signaling path\(^70\) may be different from the voice path,\(^71\) and the communications are most often encrypted.\(^72\) Because of the fact that these providers are providing similar content to users, i.e. traditional calling and messaging features, but transmitting the communications in vastly different ways, IP and VoIP service providers often are difficult to reconcile with traditional definitions of telecommunications carriers in the United States that may be present in existing legislation.\(^73\) Furthermore, some service providers may evade legislation because they are either too similar to mere broadband internet providers and cannot properly be distinguished, or because the telephone and internet services are bundled so closely that they are essentially inseparable.\(^74\)

3. The Practical Cost: System Complexity vs. System Security and Functionality

Professor of computer and information sciences at the University of Pennsylvania Matt Blaze has expressed grave concerns regarding device security and functionality, which are raised by the prospects of adding code to devices simply to comply with statutory regulations; Blaze noted that computer science technology currently, “does not know how to build complex, large-scale software that has reliably correct behavior.”\(^75\) Blaze describes in his testimony that the more code we add to a device, the more surfaces there are that leave the system vulnerable to attack, and therefore, the less secure and reliable the system becomes.\(^76\)

Consequently, adding government-mandated “backdoors” intended to provide law-enforcement access only would still weaken the overall device security because additional code must be implemented to provide that access.\(^77\)

\(^69\). See Bellovin supra note 15 at 9. Skype is perhaps the most interesting and archetypal example of this obstacle. The Skype architecture operates as a peer-to-peer network utilizing end-to-end encryption, which is much different than the traditional client-server model because Skype does not directly intercept the traffic and there are no trusted places to insert wiretap nodes pursuant to pen register orders. Id. at 10. Skype presented jurisdictional issues, as it was originally hosted in Luxembourg. Id. However, we have learned from the Snowden leaks that the NSA can in fact intercept Skype’s call and voice data and metadata. Id. at 12.

\(^70\). See Bellovin supra note 15 at 9 (“The set of links that carry the call set up messages”).

\(^71\). Id. (The actual content of the voice conversation, which is nevertheless often encrypted.).

\(^72\). Id. (This causes tapping of the “last mile connection” to be essentially pointless.).

\(^73\). See Peha supra note 65.

\(^74\). See id. at 36.


\(^77\). Id.
As we learn more about the field of computer science, we learn that additional coding does not often only interact with the code with which it is intended to interact, but rather it can affect the operation of many other systems and in many unpredictable ways—just like legislation, such as CALEA, coding does not exist in a vacuum. This can cause quite unexpected results and leave devices with unknown weaknesses, which then leave certain components exponentially more vulnerable to attacks from hackers. We cannot ignore the practical cost of government-mandated backdoors, for if devices become more vulnerable and less functional or reliable for their users, our entire technological infrastructure is likely to suffer greatly.

C. The “Crypto Wars” and Apple’s Legal Battle in the San Bernardino Case

The “going dark” debate is a phrase commonly employed to refer to growing fears surrounding law enforcement’s decreasing ability to access evidence and information necessary to execute search warrants and track down suspects. A significant portion of this debate (and, accordingly, this Note) focuses on the “Crypto Wars,” as they are often called, which particularly incite “going dark” fears as law enforcement agencies struggle to keep up with evolving cryptography and maintain surveillance over encrypted communications. Encryption has presented unique challenges for law enforcement, the most recently high-profile example of which has been the FBI’s challenge in obtaining data from an iPhone 5C owned by one of the shooters in the 2015 San Bernardino attack. Apple’s iOS 8 platform and its newer operating systems employ default end-to-end encryption, meaning that even Apple does not possess a key to the plain text versions of the communications. This constitutes a major obstacle for law enforcement agencies when they present court-ordered search warrants with which the technology provider cannot possibly comply, or at least not without additional work.

Apple’s legal battle with the FBI in the San Bernardino case is framed slightly differently from most discussion of law enforcement exceptional access and government-mandated technological backdoors. In this case, the FBI was not asking Apple to implement backdoors into its products as a preemptive measure,

---

78. Id.
79. Id.
80. See Pell supra note 9 at 605.
81. Id.
83. See Pell supra note 9 at 605.
84. Exceptional access refers to a one-way decryption key available only to law enforcement. The Obama administration was split as to whether it is advisable to mandate that technology companies provide law enforcement with a “golden key” to encrypted communications by enabling their systems with backdoors. See Apple Case Exposes Ongoing Government Rift Over Encryption Policy, 30 NO. 7 WESTLAW JOURNAL WHITE-COLLAR CRIME 6 (Mar. 18, 2016).
but rather, it was requesting that Apple create additional code after it became necessary to bypass certain security features on its encrypted devices that prevent against brute force hacking attempts.\(^5\) Specifically, Apple’s newer devices have two distinct security features designed to prevent against the possibility of hacking: (1) the devices impose escalating time delays for each incorrect attempt to enter the user’s passcode, and (2) after ten successive incorrect attempts, the device is wiped of the user’s encrypted data.\(^6\) This is especially difficult for law enforcement strategists who wish to employ brute force techniques, or government-contracted third-party hackers who seek to do the same.

Thus, the FBI requested and received a warrant and court order requiring Apple to create and implement code in its device that would disable these two security features, greatly weakening the overall security of the device and exploiting its own vulnerability, and possibly presenting an issue of user privacy invasion.\(^7\) In issuing its request, the FBI relied primarily on the fact that Apple’s help was necessary to aid in the execution of the search warrant previously issued by that court, as well as on legal authority contained in the All Writs Act\(^8\) (hereinafter the AWA).\(^9\) The U.S. District Court for the Central District of California granted the FBI’s request, ordering that Apple would do the following to allow for proper execution of the government’s warrant:

1. it will bypass or disable the auto-erase function whether or not it has been enabled;
2. it will enable the FBI to submit passcodes to the SUBJECT DEVICE for testing electronically via the physical device port, Bluetooth, Wi-Fi, or other protocol available on the SUBJECT DEVICE;
3. it will ensure that when the FBI submits passcodes to the SUBJECT DEVICE, software running on the device will not purposefully introduce any additional delay between passcode attempts beyond what is incurred by Apple hardware.

Naturally, Apple balked at this demand, and in turn the company issued a multitude of statements vigorously denouncing the FBI’s request, eventually leading to the FBI’s filing of a motion to compel\(^1\) the company to comply with the order.\(^2\) Ultimately, the legal battle between the FBI and Apple over access to the San Bernardino gunman’s iPhone ended rather anticlimactically. The FBI

\(^5\) See Pell supra note 9 at 605.
\(^6\) Id.
\(^7\) In re An Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, No. ED 15-0451M, 2016 U.S. Dist. LEXIS 20543 (C.D. Cal. Feb. 16, 2016) [hereinafter In re Apple iPhone].
\(^9\) See In re Apple iPhone, 2016 U.S. Dist. LEXIS 20543.
\(^1\) Id.
\(^2\) The entire text of the motion is available at http://www.politico.com/f/?id=00000152-fae6-d7cd-af53-fafe53bb0002.
\(^2\) See Jordan Novet, Apple vs. FBI: A Timeline of the iPhone Encryption Case, VB (Feb. 19, 2016 8:47 PM), http://venturebeat.com/2016/02/19/apple-fbi-timeline/.
eventually employed third-party hackers to access the encrypted communications and dropped its court action against the technology giant.\textsuperscript{93} Therefore, the outcome of this action is far less influential on the overall “going dark” debate and the “Crypto Wars” than the policy and legal arguments made therein, the statutory authority invoked, and the impact that they have had on discourse surrounding encryption access issues.

III. ARGUMENTS IN FAVOR OF DECRYPTION “GOLDEN KEYS” FOR GOVERNMENT AND LAW ENFORCEMENT

While the battle over the San Bernardino iPhone may have ended, the policy arguments espoused in favor of exceptional access for law enforcement, i.e. one-way “golden keys” provided only to the government to decrypt communications, were only beginning to emerge. It was apparent that the FBI did not intend to back down in its policy fight for increased access to Apple’s devices, regardless of its motion to vacate its order to compel the company to create the requested code in the California case.\textsuperscript{94} In a related proceeding in the U.S. District Court for the Eastern District of New York, the FBI continued to assert that Apple should be required to assist it in enabling the search of a device for which the court had previously issued a warrant.\textsuperscript{95}

It logically follows that the FBI’s request in this case was backed by the district court’s previous issuance of the search warrant, but the invocation of the AWA as justification for the demand on Apple is an interesting attempt to engage broad statutory language to convince the court to grant the FBI’s request. The current language of the relevant section of the AWA as invoked by the FBI reads as follows: “The Supreme Court and all courts established by Act of Congress may issue all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of law.”\textsuperscript{96} Truly, this language is so broad that it is hard to imagine an argument that could not be made which applied it to any factual scenario, and this was precisely the FBI’s somewhat of a shot-in-the-dark attempt to convince the court to grant its demand of Apple.

Because legal scholarship on encryption technology is still in its nascent phase, there is little existing legal authority to justify the government’s request, and the AWA may be, under these circumstances, a reasonable attempt to compel Apple’s assistance. To structure its analysis of this argument, the court isolated three criteria which must be met in order to apply the AWA: (1) the writ must be

\begin{itemize}
\item \textsuperscript{94} \textit{In re Apple iPhone}, 2016 U.S. Dist. LEXIS 20543.
\item \textsuperscript{95} See \textit{In re Order Requiring Apple, Inc. to Assist in the Execution of a Search Warrant Issued by this Court}, No. 15-MC-1902 (JO), 2016 U.S. Dist. LEXIS 25555, at *1-96 (E.D.N.Y. Oct. 9, 2015).
\item \textsuperscript{96} 28 U.S.C. § 1651(a) (1948).
\end{itemize}
in aid of the issuing court’s jurisdiction, (2) the type of writ requested must be necessary and appropriate in furtherance of the aid to the issuing court’s jurisdiction, and (3) the writ must be agreeable to the usages and principles of law.”

Because these are rather basic requirements, even if all three are satisfied, the court may consider an additional three factors in exercising its discretion as to whether to issue the writ or not. The district court recalled the Supreme Court’s dicta in *U.S. v. N.Y. Tel. Co.* addressing the three critical considerations in this regard: (1) the degree of relation between the person to whom the writ is being directed and the subject matter of the court’s jurisdiction, (2) the reasonableness of the burden the writ would impose, and (3) the necessity of the writ in the aid of the matter of jurisdiction.

The New York court concluded that the AWA did not authorize such a writ under these circumstances. In a memorandum opinion, the magistrate judge held that the request did not satisfy the last of the three statutory requirements, namely that the writ be agreeable to the usages and principles of trade. He found that the constitutionality of the AWA could not be maintained if the court were to adopt the FBI’s exceedingly overbroad proposed interpretation of the Act. The judge further stated that, even if all three requirements had been met, he would deny the writ as a matter of discretion. The government agencies and law enforcement may have very reasonable and practical fears that their decreasing technical abilities to access data legally obtained through a court-ordered warrant obstructs essential evidence and stalls crucial investigations. However, the use of broad statutory authority, even coupled with these practical policy arguments, have not proved effective enough legal tools in the battle against “going dark.”

**IV. IN OPPOSITION TO GOVERNMENT-MANDATED BACKDOORS**

While the side of this debate in favor of exceptional access often characterizes its position as one of increased “security,” for our nation, it could be argued that security is perhaps a greater risk if exceptional access for law enforcement were to be granted. Of course, this argument employs the use of the term “security” in a slightly different sense, as it refers to the cybersecurity of our technological infrastructure. In favor of Apple, several arguments were raised by various groups, ranging from civil liberties groups to technology developers, providers, and manufacturers. These groups articulated policy concerns,
cybersecurity threats, and civil liberties violations that might be implicated by the
government’s potential mandates for backdoors into encrypted communications.

An independent company, Lavabit LLC, submitted an amicus curiae brief on
behalf of Apple in the California proceedings.\textsuperscript{104} In its brief, Lavabit argued that
the AWA did not authorize such an extraordinary measure as the FBI requested
of Apple, which it claimed was significantly more invasive of Apple’s privacy
and security than a simple pen register order.\textsuperscript{105} The company argued that the
circumstances in this case were not so extraordinary as to justify the possibility
of compromising Apple’s operating services and intellectual property.\textsuperscript{106} Lavabit
further alleged numerous constitutional violations, including violations of
Apple’s First Amendment right to free speech and its Thirteenth Amendment
right to be free from involuntary servitude.\textsuperscript{107} Finally, the company argued that it
was unduly burdensome to require Apple to undermine and weaken its own
security, for which it has come to be known among technology consumers.\textsuperscript{108}
Lavabit asserted that it was unfair and uncalled for under the circumstances to
require Apple, an innocent technology company, to enable the investigation at
the expense of its own proprietary interests.\textsuperscript{109}

Additionally, two major policy considerations are implicated by the FBI’s
demand. First, many have expressed concern about the proposed overbroad
reading of the AWA and what further investigative actions it might be invoked to
compel.\textsuperscript{110} In the face of an uncertain, yet potential, surge in surveillance-
enabling mechanisms and requirements, there is legitimate concern that the
public might become fearful of the government’s intervention with their personal
devices. Such widespread fear would likely be detrimental to our technological
infrastructure in its entirety.

To this effect, Dr. Christopher Soghoian, a technologist experienced with
cybersecurity issues, has suggested that increasing consumer fear of government-
mandated surveillance mechanisms could have an extremely adverse effect on
our technology infrastructure.\textsuperscript{111} Soghoian compared software updates for our
computers to vaccines; he argues that both are regularly necessary for the health
of the entire community, for if a few in the community are afraid to vaccinate (or
enable software updates), then the group as a whole is more vulnerable to threat

\textsuperscript{104}. See Brief in Support of Apple Inc.’s Motion to Vacate, In re Apple Iphone, 2016 U.S. Dist.
LEXIS 20543 (No. 5:16-cm-00010-SP-1), 2016 WL 1134139.
\textsuperscript{105}. Id.
\textsuperscript{106}. Id.
\textsuperscript{107}. Id.
\textsuperscript{108}. Id.
\textsuperscript{109}. Id.
\textsuperscript{110}. See Pell supra note 9 at 614-15.
\textsuperscript{111}. See id. at 615 (citing Christopher Soghoian, The Technology at the Heart of the Apple-
of-the-apple-fbi-debate-explained.)
of disease (or identity theft and cyber attacks).\textsuperscript{112} Apple and others argue that creating new vulnerabilities in software, or exploiting existing ones, would be harmful to our national security if individuals are able to then hack into the devices more easily and at a greater rate.\textsuperscript{113}

Second, in light of the FTC’s advocacy of strong encryption use to protect sensitive user data, it seems paradoxical and misleading for another arm of the federal government to then impose both strict limitations on developer’s innovation abilities and substantial burdens upon the security and functionality of their systems.\textsuperscript{114} Subjecting entities that use technology to protect user information to contentiously conflicting guidance from multiple branches within our federal government, as well as harsh penalties for data breaches and information leaks, seems like a sure method of driving away some of our most profitable and innovative corporations. Furthermore, when this state of affairs is coupled with the cybersecurity threats associated with requests for exceptional law enforcement access, it can only be a matter of time before technology giants such as Apple and Google grow tired of expending resources to out-maneuver the federal government whenever a novel case arises.

V. A REJECTION OF EXCEPTIONAL ACCESS AND A REVIEW OF PROPOSED ALTERNATIVES

A. The Dangerous Fiction of Law Enforcement’s “Golden Key”

In theory, it seems ideal to provide the government in warranted situations with a privately accessible key, i.e. a confidential input value that will allow the government agency to yield the correct output from the cryptographic algorithm to decrypt the communication into readable format. However, in practice, there is no such thing as a golden key available only to the “good guys,” while all others are entirely unable to interact with the additional coding required to provide that elite access. Professor Matt Blaze has consistently advocated that there are no such things as lawful access only mechanisms that would ensure backdoors for law enforcement could be coded into software, yet somehow remain inaccessible to hackers and identity thieves.\textsuperscript{115} The consensus among technology experts seems to be that any additional coding that would allow law enforcement access would also leave the system more vulnerable to a number of other, possibly

\textsuperscript{112} See id.

\textsuperscript{113} Id.


\textsuperscript{115} Exceptional access for law enforcement has been referred to as a “dangerous fiction that threatens to undermine our national and economic security.” See Pell supra note 9 at 607.
unknown and unexpected, security risks. Blaze illustrates this point with a telling example from recent national history.

In 1993, the NSA designed a security device referred to as the “Clipper chip,” which could be inserted into systems that encrypted data. While this encryption chip was praised for its stronger encryption algorithm, it was criticized for its feature allowing a key to Clipper-encrypted data to be held in escrow by the government; if the government were to need the data to execute a warrant, it could retrieve the key and decrypt the information. While there were natural privacy and surveillance concerns that arose within the general public, additional security concerns were also at issue with the device. Blaze noted that there were a number of security flaws, unknown at the device’s inception and introduction, that severely compromised its security, “one of which made it possible for a rogue user to bypass the government access feature while still making use of the encryption algorithm.” Blaze even published a practical guide to this hack in order to demonstrate the device’s lack of security.

In a perfect universe, it would be viable to provide law enforcement with a decryption “golden key,” which could only be accessed pursuant to a court-issued warrant, but could not under any circumstances be accessed by unauthorized third-party hackers, nor would the functionality of the device(s) be compromised in any way by additional coding. This would be ideal for all parties to the “going dark” debate, to be sure. However, this is simply not a technological reality. The U.S. cannot afford technologically or economically to forestall the inevitable and continue to place outdated and undue burdens on our most technologically advanced companies with respect to cryptography policy. To express the same sentiment a bit differently, we cannot continue this existing paradox in which we (1) encourage our most innovative and engaged corporations to use encryption to vigilantly protect user data at the outset, (2) punish them harshly for security breaches in which they failed to use strong enough encryption algorithms, and then (3) simultaneously subtly limit encryption by requiring backdoors that are costly to the companies in terms of functionality, security, and economic return. The current state of affairs defies all logic and is unconducive to fostering economic and technological growth.


118. Id.

119. Id.

120. Id.

121. See id.

122. See id.
The federal government is sending very mixed signals, likely because our nation has not yet developed a concrete stance on encryption regulation, but it could potentially have detrimental effects in the long-term practical reality in a very short period of time. Mixed signals and uncertain, unfavorable laws and policy changes are surely not the most effective means of keeping corporations, such as Apple, Google, and others, within our economic grasp. If the United States chooses to alienate technologically innovative businesses with restrictive laws that ultimately reduce device security, functionality, and reliability, then it ignores the reality of our technology-driven global economy. While aid of law enforcement is of course a necessary and noble goal, the burden ought not be on technology companies and communications providers, who are essential to national commerce, and who have a duty of data and privacy protection to those customers whom they serve.

B. Alternative Responses to “Going Dark” Concerns

While government-mandated backdoors to enable the execution of all search warrants might be the simplest and easiest route, and naturally the hope and desire of law enforcement agencies, it is for the foregoing reasons that it is simply not technologically sustainable considering legitimate cybersecurity concerns. In its place, multiple solutions have been proffered, a combination of which in many circumstances could allow law enforcement to glean the same degree of information as a policy of exceptional access and mandated backdoors and allay some of the “going dark” concerns. Two solutions that have been suggested are: (1) enhanced collection of metadata from Internet of Things (IoT) devices, and (2) greater investment in the government’s own “lawful” hacking capabilities. Of these two means of addressing the issue, use of the IoT is the significantly weaker option, as it presents its own privacy issues and is limited in scope. However, increased user interaction with the IoT could aid law enforcement access endeavors in conjunction with lawful hacking efforts.

1. The Internet of Things (IoT)

The IoT refers to objects around us in daily life that are increasingly gaining wireless connective capabilities. These could be speakers, cameras, car components, etc. that connect to the internet and track and store data on their users’ activities. These things reveal valuable metadata, which exceptional access opponents advocate as a wealth of information about an individual that

123. See generally Joseph Menn & Dustin Volz, Apple Case Exposes Ongoing Government Rift Over Encryption Policy, REUTERS (Mar. 7, 2016 7:29pm EST), http://www.reuters.com/article/us-apple-encryption-schism-insight-idUSKCN0W70U5 (noting that, while the Department of Justice and the FBI have endeavored to convince other federal departments and agencies to join the fight against unbreakable encryption, it has perpetuated more interagency debate than consensus).
124. See Pell supra note 9 at 629.
125. Id.
could replace the need for technological backdoors, conveying much about the user’s life and daily habits.\footnote{126. Id.} Some argue that this would allow the government to “design individualized investigative plans for targets based on the kinds of devices they use and the kinds of metadata or public source content (think Twitter and Facebook) such devices and services reveal,” which could be an effective alternative to imposing strict mandates on technology developers and manufacturers.\footnote{127. Id. at 632.}

The IoT opens a wide arena of information-gathering possibilities that could be afforded to law enforcement. In theory, any network-connected device that has audio or video capability could be used to spy on a suspect’s communications, or a device could be used to access the user or network credentials of another device belonging to a suspect to obtain further information about the individual.\footnote{128. Id. at 634.} Such information would provide great insight into the daily activities and behavior of suspects, beyond simply gathering information from encrypted communications. James Clapper, the Director of National Intelligence, expressed the expansive information-gathering potential of the IoT, noting that “in the future, intelligence services might use the IoT for identification, surveillance, monitoring, location tracking, and targeting for recruitment, or to gain access to networks or user credentials.”\footnote{129. Id.} In a January 2015 FTC Staff Report, the Commission noted that there would be 25 billion IoT-connected devices that year, which was expected to double to 50 billion by the year 2020.\footnote{130. See Pell supra note 9 at 629.}

However, it is important to note that the bounds of federal access possibilities stemming from the IoT would not be limitless. The Ninth Circuit addressed the scope of this sort of access in Company v. U.S., in which the court considered whether a car’s onboard driver assistance technology could be used to record conversations occurring within the car because such use would completely disable essential features of the system.\footnote{131. Co. v. U.S., 349 F.3d 1132, 1149 (9th Cir. 2003).} Looking to Title III of the Omnibus Crime Control and Safe Streets Act,\footnote{132. Omnibus Crime Control and Safe Streets Act, Pub. L. No. 90-351, Title III, 82 Stat. 197 (1968). The text of Title III of the Act is available at https://it.ojp.gov/PrivacyLiberty/authorities/statutes/1284.} the court discussed whether the wiretapping authority extended to these circumstances.\footnote{133. Id. at 1136.}

The court ultimately concluded that the complete disabling of the car’s onboard system violated the “minimum interference” requirement of the Act, and therefore the wiretap warrant could not be sustained in such a situation.\footnote{134. Id. at 1146.}
Ultimately, the government surveillance of IoT devices presents similar privacy and security concerns to those raised in response to the FBI’s demands of Apple. Additionally, while metadata obtained from IoT devices is useful in many ways, it is not the same as the ability to decrypt suspect communications. Therefore, while the IoT presents new information tracking possibilities, it cannot solve the problem alone.

2. “Lawful” Hacking

Many technology experts, such as Professor Blaze, suggest that the government has not carried its burden in devoting time and resources to development of its own “lawful” hacking abilities. In the aftermath of the resolution of the California Apple case, Blaze commented, “The fact that the FBI had to go to a third party indicates that the FBI either had or devoted insufficient resources to finding a solution.” There are plenty who believe that the government could, and should, be doing more in the way of “lawful hacking.” In a jointly authored article by Professor Matt Blaze and fellow information technology expert Steven Bellovin, the pair asserts that an adequate understanding of how to exploit existing vulnerabilities in software would render an extension of CALEA’s mandates wholly unnecessary. Once the target has been identified and obtaining the information has been authorized by a warrant, the article suggests that a “lawful hacker” search for an easy-to-influence vulnerability, considering such pressing factors as compatibility with the user’s operating system (to enter and infect it), and mode of delivery (email, USB device, etc.). While this is not an easy task, the Blaze and Bellovin maintain that it is certainly possible under most circumstances, and, under all circumstances, still preferable to mandated backdoors which would weaken security mechanisms.

The concept of “lawful” hacking necessarily implicates a few key issues, primarily the legal requirements to obtain proper authorization for the specific interception, the ethical concerns in exploiting programming vulnerabilities in the name of protecting technology, and the cybersecurity repercussions of promoting hacking activities. In order to maintain the integrity of the Fourth Amendment and its warrant requirement, Bellovin and Blaze note that perhaps two distinct
court orders would be required to provide sufficient authority for a complete data collection.141 First, authority would need to be granted for the hacking of the personal device, and then, secondly, permission would need to be obtained for the requested interception of information.142 One example of a legal means by which the government previously obtained proper authorization for such hacking consisted of first obtaining a search warrant to install software on the target device, which would transmit information back to the FBI, and then requesting a pen register/trap-and-trace order to elicit the desired information.143

The practical mechanics of this system lie in either purchasing off-the-shelf, black-market exploitation software to access devices, or paying for a specific solution through a third-party or federally-employed computer science researcher.144 It may be noted that the latter would likely be more effective in a time-sensitive case in which law enforcement is looking to quickly access one component of a target device.145 There is an emerging and increasing market for exposing such exploitation capabilities, with private companies146 selling subscriptions for such services for as much as $100,000 annually.147 Naturally, this gives rise to some ethical misapprehension; one would say that it best furthers a policy of data protection to report and patch system vulnerabilities, not exploit them, especially for profit on an open market. The intervention of the government into the world of “lawful” hacking would only expand the market for sale of such information. At its most extreme, it could be postulated that federal law enforcement agencies might even discourage communications or software providers from patching vulnerabilities to maintain access in certain circumstances.148 While “lawful” hacking is a viable alternative in many ways, the ethical concerns cannot be ignored, as they will most certainly evolve as government intervention in hacking technology increases.

Finally, there are serious security concerns that arise when existing vulnerabilities, likely unknown to the software developer, are discovered and exploited by government agencies or third-party hacking companies. How may the information be used, and how can the government successfully limit its access to the minimal intrusion necessary as it is required to do? Furthermore, and most seriously, should the developer as a matter of right receive notice and detail of the existing vulnerability once it is discovered? These issues are complex and constantly evolving, requiring a continuing dialogue about the limits and restraints on such exploitation of technological vulnerabilities.

141. See id. at 31.
142. Id.
143. Id. at 32.
144. Id. at 41.
146. Id. at 42. (Examples of such companies include Vupen, Revuln, and Vulnerability-Lab.)
147. Id.
148. Id. at 48.
Two preliminary issues address the potential dangers that the law enforcement agency will collect more data than is authorized by its warrant, or that its authorized exploit will have unintended consequences in the target system. This could present complications in the judicial process, as decisions on whether specific exploits could be used to execute a previously-authorized warrant would have to be a secondary question determined by courts prior to allowing law enforcement to implement the desired exploit on the target device. The primary concerns in this respect are (1) that the law enforcement agency does not exceed its authority under the issued warrant by receiving unauthorized communications or data, and (2) that the agency does not surpass the standard of minimum interference permitted by the Wiretap Act.

Ultimately, however, the most pressing security concern presented by a concept of “lawful” hacking is whether the discoverer of the vulnerability would be required to report it to the government or to the developer. In an ideal world, one might hope that every vulnerability would be immediately reported, to both the developer and the public. Bellovin and Blaze state that this is a viable option because the amount of vulnerabilities is infinite, so if vulnerabilities are discovered and exploited at faster rates than they may be patched and repaired, the government is not impeded in exploiting useful vulnerabilities where authorized. One subsequent issue, however, is that of compensation and incentive. While it may be most beneficial for federal or third-party hackers to reveal their discoveries immediately to the developer and to the public as a matter of right, they would likely lack incentive to do so. Furthermore, there is the issue of the compensation rates and incentives provided by the federal government to those “legal hackers” whom it employs would be great enough to attract and retain the strongest emerging IT minds.

Fittingly, this precise issue has been relatively recently raised regarding the FBI’s use of a third-party hacker to exploit the desired vulnerabilities in Apple’s operating system on the San Bernardino shooter’s iPhone 5C. On September 16, 2016, it was released that the Associated Press, joined by two other media outlets, has initiated a lawsuit against the FBI seeking to obtain disclosure of whom the agency paid and how much it spent to access the encrypted

---

149. Id. at 50.
150. Id.
151. Bellovin supra note 15 at 56.
152. See id.
communications. While FBI Director James Comey has released a few details about the transaction, including that it cost the FBI more than he will earn in his position as long as he remains employed, the details of the exploit have not been disclosed by the agency. The current suit, filed in the District Court for the District of Columbia, arises under the U.S. Freedom of Information Act and will likely have a significant impact on legal policy considerations regarding who may receive information of discovered vulnerabilities. Although the concept of “lawful” hacking implicates many policy considerations of its own, they do not abrogate the value that such hacking opportunities might provide for law enforcement. Rather than focusing our national discourse on policy concerns surrounding expanding wiretap authority and implementing mandatory “backdoor” legislation, perhaps it would be more fruitful to center discussion on the potential use, and potential limits, of a “lawful” hacking solution to “going dark.”

VI. CONCLUSION

In recent years, the use of encrypted communications services has inhibited the ability of law enforcement agencies to intercept information needed as evidence in investigations, for which a valid warrant has been issued. The government has sought the cooperation of technology developers and manufactures in enabling the executions of these warrants, and have met more than a degree of reluctance from the technology companies in doing so. Previous legislation to enable government access, such as CALEA, is now becoming obsolete in the face of advancing technology. The question arises, then, as to whether such legislation should be expanded, or, in the alternative, whether other access options should be explored. While law enforcement claims that exceptional access to warranted communications is necessary to the security of our nation, many corporations and data privacy advocates disagree. Technology companies, civil liberties unions, consumers, and cryptography experts have expressed a variety of concerns with demands like those the FBI attempted to impose upon Apple, ranging from privacy infringement to the damaging of our technological infrastructure.

Considering such competing concerns, it seems most prudent that law enforcement, at least for the time being, explore alternative routes of receiving the necessary information or accessing the encrypted communications. The current state of conflicting national cryptography policy guidance, as well as ongoing high-profile litigation involving major technology corporations, is problematic for the U.S. in its pursuit to not only remain globally competitive in the way of technology, but to be among the most technologically innovative nations in the world.

155. See Eric Tucker supra note 153.
156. Id.
157. Id.
nations in the world. To achieve this, in a practical sense, the U.S. must also be a pioneer in data security.

This is an exceedingly complex issue because it produces impact on such an expansive scale, from individuals and their personal devices, to mid-level or even large communications service providers, to multi-national technology corporations like Apple, or Google, and finally, to the relative positioning of the U.S. within the global economy. Discussion of issues surrounding cryptography necessarily require such a multi-tiered analysis to assess the impact on each of these levels. Most importantly, such discussion must be framed in terms of U.S. policy positioning on a global scale, as the U.S. has certainly yet to corner the market on technological innovation. It seems that placing our most technologically innovative corporations in a perilous legal limbo regarding encryption policies can only be anticipated to produce negative results.

While there is currently no perfect alternative to government-mandated backdoors, the most effective solution is likely some combination of IoT investigation, with its prospect of rich metadata collection, coupled with improved and expanded federal “lawful hacking” techniques. If most experts agree that no platform is entirely secure, and that all have vulnerabilities in some capacity or other, then it seems only sensible that, in such situations as those the FBI faced with Apple in recent years, law enforcement seeks to identify and exploit these vulnerabilities to obtain the necessary information. However, this suggestion does compel one serious future consideration: whether the technology companies should be furnished as of right with the results of these attempts by law enforcement agencies. While we should theoretically strive to encourage cooperation between our most technologically advanced corporations and federal law enforcement agencies, the adversarial atmosphere created by the competing legal and cybersecurity interests has already proven to be difficult to overcome in practice.
THE COMPUTER FRAUD AND ABUSE ACT: PUNISHING HACKERS AND SOLVING EMPLOYMENT DISPUTES IN THE SAME STATUTE

Rob Spicer*

I. INTRODUCTION

The Computer Fraud and Abuse Act ("CFAA"), an amendment to the Comprehensive Crime Control Act of 1984, was the first legislation put in place to criminalize computer hacking in the United States.¹ This legislation criminalized hacking regardless of intent or result.² The CFAA has had eight amendments from 1988 to 2008, and not a single one has addressed the consequences that independent security researchers face under the act.³ In fact, security researchers are not only subject to criminal and civil liability under the CFAA, but also under other acts, such as the Electronic Communications Privacy Act ("ECPA"), and the Digital Millennium Copyright Act ("DMCA").⁴ While the original design of the CFAA was primarily a criminal statute, anyone who suffers damage or loss may now bring a civil action to court.⁵ Additionally, the CFAA has no specific intent requirement, indicating that the damage or loss suffered does not need to be intentional.⁶

Independent security research is important in order to protect consumers. For instance, the tech-giant Google has been known to supply grants and rewards for independent security researchers to encourage them to help find vulnerabilities in their own products.⁷ In 2015, two researchers found security flaws in Chrysler cars that would allow a hacker to gain access to the car.

---
* Rob Spicer, 3L J.D. Candidate, NKU Salmon P. Chase College of Law, Class of 2018.
2. Id.
3. Id..
6. Id.
remotely through the internet. Organizations such as the Electronic Frontier Foundation have advocated for researchers to have the right to search for vulnerabilities without fear of prosecution, and have asked congress for DMCA exemptions. On October 28, 2015, Congress announced ten exemptions under the DMCA, including a vehicle software exemption. These exemptions will last for three years and are fairly narrow. While the exemptions are a positive step, the process of getting exemptions is tedious, and many areas will not be covered by one of the ten exemptions.

Although the exemption process under the DMCA may not be ideal, it is still a step in the right direction, whereas the CFAA has had no exemptions, and, over the course of its amendments, has actually become stricter and penalties made more severe. A major issue is that corporations can actually impose their own rules under the CFAA through their terms of service. The federal courts have addressed many issues with the CFAA including the interpretation of phrases such as “exceeds authorization.” There exists a circuit split when interpreting the CFAA and use restrictions imposed by the owners of the software or computers in general. The decisions of this split deal with employer and employee relationships and when the employee violates a company computer use policy. The conflicting interpretations of the circuits raises the question of how far the CFAA can go in employer and employee relationships, and if it is even dealing with hacking at a certain point. If the CFAA is going to be used in employment disputes going forward, then a uniform interpretation of the statute is required.

The CFAA has faced scrutiny for the overly harsh penalties associated with it. In 2015, a proposed amendment to the CFAA, known as Aaron’s Law, was

9. Id.
11. Id.
12. Id.
14. Id.
18. Id.
reintroduced to congress, but has not been voted on.20 The amendment was named after Aaron Swartz, who was prosecuted for downloading academic materials with the intent to distribute them.21 While no financial damage was incurred, and no civil suit was filed, the federal government pursued a criminal case against him, with the possible penalty of a 35-year prison sentence.22 Tragically, during the legal battle, Aaron was found dead from a presumed suicide, which spurred discussion of reducing the harsh punishments of the CFAA for similar cases.23 The proposed text of the bill sought to clarify the “access without authorization” language of the CFAA, and to adjust the penalties of the crimes.24

While these proposed amendments have not been accepted, the CFAA needs to be revamped as it applies to many citizens on a daily basis.25 With the technological leaps that have been made over the past few decades, it seems unlikely that over thirty years ago the drafters of the CFAA could predict how it would be applied today.26 In this note a brief history of the CFAA will be discussed, along with the current circuit split, followed by an examination of how the split has created uncertainty for professional researchers as well as how the statute is being used in the employment setting, relating less and less to hacking. Between inconsistent interpretations, security risks, and misuse in employment relationships, the CFAA needs to be replaced, or at the very least, the narrow interpretation should be adopted uniformly.

II. BACKGROUND OF THE CFAA AND CURRENT SPLIT

A. Background

The CFAA is codified as 18 U.S.C. § 1030 and covers conduct by a person who knowingly or intentionally “accesses a computer without authorization or exceeding authorized access.”27 The Comprehensive Crime Control Act was first passed in 1984, and Congress expanded the statute in 1986 with the CFAA amendment, even though the entire statute is commonly referred to as the CFAA.28 The CFAA originally only provided criminal penalties, yet in 1994 Congress passed an amendment that allowed for private parties to pursue civil causes of actions.29

20. Id.
21. Id.
22. Id.
23. Id.
25. Pyne, supra note 16.
26. Id.
27. 18 U.S.C. § 1030.
28. CFAA Background, supra note 15.
29. Id.
Through subsequent amendments the CFAA continued to broaden. The Economic Espionage Act expanded the statute in 1996, changing the financial records section to encompass any information of any kind involving interstate or foreign communication, changing the phrase “federal interest computer” to “protected computer,” and increased penalties in several sections. With the USA Patriot Act, “protected computers” no longer included only domestic machines, but those outside the United States, while again increasing penalties. Finally, in 2008, another amendment also broadened the definition of a threat and of a “protected computer” and imposed stricter penalties for acts falling under the statute. Under this definition of “protected computer,” the statute utilizes the Commerce Clause power of the Constitution and attempts to reach as far as possible. Under this standard, it could be argued that any device connected to the internet would a protected computer.

High profile cases, such as the death of Aaron Swartz as mentioned previously, have brought the public’s attention to these stricter penalties. The case brought against the “PayPal 14” for their hacktivism acts in 2010 was another such high profile case. Hacktivism is generally defined as a type of activism, mixing elements of technology with the ideas of protesting. A simple definition of hacktivism would be hacking for a political or socially motivated purpose. In 2010, a group of hackers led by Anonymous utilized a serious of denial-of-service (“DDoS”) attacks against several financial institutes, including PayPal. These DDoS attacks flooded the institutes’s servers with false traffic, which interrupted service for anyone else attempting to access the sites. The PayPal 14 did this to protest the companies’ refusal to process payments to WikiLeaks, the organization known for publishing classified documents and exposing news from anonymous sources.

---

30. Id.
31. Id.
32. Id.
33. Id.
34. CFAA Background, supra note 15.
35. Reader, supra note 19.
41. Charges dropped, supra note 36.
While these individuals who were being prosecuted did not deny their involvement, the Government initially sought sentences of up to ten years in prison and fines of up to $250,000. These types of penalties spurred debate on the trial, with people expressing concerns that the CFAA does not differentiate between mere civil disobedience and malicious attacks. Ultimately, prosecutors negotiated plea bargains with the individuals in which they owed $5,600 in restitution, and either were placed on probation or served ninety day jail sentences, a far cry from the original sentencing discussed. This incident illustrates the problem with equating protesting with malicious hacking, and the need to be able to differentiate the two. However, the ability to charge all computer violations the same is not the only problem with the CFAA.

The CFAA also has also created interpretation issues as evidenced by the disagreement between the circuit courts. The phrase “exceeds authorized access” has been interpreted by the circuit courts to have different meanings under the CFAA. Specifically, courts have come to different conclusions when analyzing authorized access and how it applies to terms of service (“ToS”) agreements, and computer-use policies put in place by employers, or even software designers or website administrators. While the CFAA defines what a computer is, it does not define authorization and courts have the opportunity to define exceeding authorized access as simply violating a website’s ToS. This is problematic as virtually all websites that are used by consumers have a ToS, with their own rules. Not surprisingly, as most individuals use social media in some form, most individuals are also bound by a ToS created by a social media company. If one were to violate the ToS of a particular website, should he or she be subject to all the punishments that the CFAA provides? Some of these terms are violated regularly, such as dating websites prohibiting inaccurate or misleading information. Even if government agencies were to promise not to pursue minor violations, it would be in their power to do so if they deemed fit.

What if one of these minor violations led to a tragic event? Would the government be able to pursue the minor violation then? When Lori Drew was indicted, she was charged under the CFAA for a violation of the ToS of social media site, MySpace.com. MySpace is a social networking site that allows

42. Id.
43. Eördögh, supra note 40.
44. Id.
45. Id.
46. Pyne, supra note 16.
47. Id.
49. Id.
51. Id. at 862.
users to create profiles, and then use those profiles to interact with other users.\footnote{88} The indictment indicated that Drew exceeding authorized access under the CFAA by creating a fictitious MySpace profile, and assuming the identity of a sixteen-year-old male.\footnote{53} Using this fake profile, Drew tormented a thirteen-year-old female by manipulating her emotions and the young girl eventually killed herself.\footnote{54} After the teen had killed herself, Drew then deleted the fake MySpace profile.\footnote{56}

MySpace had a ToS that was inherently agreed upon by the creation of a profile. The issue raised by this tragic case was whether a violation of these terms was, in fact, a violation of the CFAA.\footnote{57} MySpace had terms that prohibited a user from posting certain material, such as material that was offensive, racist, bigoted, or material that harassed another person.\footnote{58} Drew’s violation of terms included using a photograph of another person without consent, soliciting personal information from a person under the age of eighteen, providing information that is false or misleading, and several others.\footnote{59} However, the Court noted that if the CFAA provided punishment for every ToS violation, then every website owner would be defining criminal conduct.\footnote{60} Additionally, interpretation would become a problem as well, because if the ToS were written vaguely or in an over-encompassing way, then there would be more problems applying punishments.\footnote{61} Finally the Court held that the element of scienter had to be applied to the intent requirement of the CFAA because if it did not, there would be no limitation to what kind of breaches would be criminally prosecutable.\footnote{62} This last element is the fear that many individuals, including security researchers, hold when conducting their work, as researchers intentionally break the ToS, but with the purpose of either creating a safer environment or studying the implications of algorithms.

\section*{B. Narrow Interpretation of the CFAA}

While \textit{United States v. Drew} supports a narrow interpretation of the CFAA in the context of ToS violations, the federal judicial circuits are not in agreement. For instance, the Ninth Circuit, Second Circuit and Fourth Circuit have adopted a narrow view of the CFAA.\footnote{63} The First Circuit, Fifth Circuit, Seventh Circuit, and

\begin{thebibliography}{99}
\item 53. Id. at 453.
\item 54. Id. at 452.
\item 55. Id.
\item 56. Id.
\item 57. Drew, 259 F.R.D. at 457.
\item 58. Id. at 454.
\item 59. Id. at 461.
\item 60. Id. at 465.
\item 61. Id.
\item 62. Id. at 467.
\end{thebibliography}
Eleventh Circuit have adopted broad views of the CFAA. The Circuits’s use restriction interpretations have surfaced in employer-employee relationship cases when determining whether an employee has exceeded authorized access when using company computers and networks. Like a website’s ToS, employees generally accept computer use policies in exchange for being able to use the company’s database or resources. The following will briefly describe these courts interpretations of the CFAA.

The Ninth Circuit’s interpretation is found in United States v. Nosal. Ex-employee David Nosal convinced some of his former co-workers, who were still employed with his old company, to create a competing business. In order to create this business, the co-workers used their access to the company database to download source lists, names and contact information and then gave that information to Nosal. The issue in this case arose as the co-workers were still employees at the company, and as such did have access to the company database, but the company had a computer use policy that forbade disclosing confidential information. In regard to the CFAA charge, Nosal argued that the statute is only in place to target hackers, and not an individual who had access, yet violated a computer use policy.

In its opinion, the Court pointed out that a broad interpretation would cause harmless activities to turn into federal crimes by only using a computer to complete them. For instance, if a company had a policy that an employee’s work email could not be used for personal contacts, then an employee would be punished for emailing a family member as opposed to calling the family member and delivering the same message. If the company has a policy that prevents a user from visiting websites for pleasure, the user would be punished for visiting popular sporting websites to read news, but not punished for bringing in a physical copy of the sports section. In other words, many of the activities that employees regularly participate in at work – reading news articles, communicating with family, completing crosswords or puzzles, or anything else that may be done aside from work – suddenly become federal crimes under the CFAA if done on a computer at work.


64. Id.
65. Id.
66. Nosal, 676 F.3d at 854.
67. Id. at 856.
68. Id.
69. Id.
70. Id.
71. Id. at 860.
72. Nosal, 676 F.3d at 860.
73. Id. at 860.
74. Id.
The Court also briefly discussed ToS agreements on websites, and how enforcing those through the CFAA would create additional problems.\textsuperscript{75} Websites that require children to be of at least a certain age would find many guilty juveniles, with adults as their contributors.\textsuperscript{76} Many websites don’t allow accounts to be shared, yet sharing email, or other personal accounts, between family members is a very common practice, and this would make all these individuals culpable under the CFAA.\textsuperscript{77} Dating websites prohibit misleading information, yet it is common practice for individuals to exaggerate their positive features, which also would be held to be criminal.\textsuperscript{78} But perhaps the most chilling conclusion of accepting a broad interpretation of the CFAA would be that each of these websites would be able to change their ToS at any time, creating new punishable activities on a whim.\textsuperscript{79}

On a similar set of facts as \textit{United States v. Nosal}, the Fourth Circuit examined the CFAA’s applicability to an ex-employee who provided a competitor proprietary information that he downloaded from the company’s database.\textsuperscript{80} Mike Miller originally worked for a company that provided him with a laptop computer and a cellphone while additionally authorizing his access to the company databases that held numerous confidential documents.\textsuperscript{81} The company had policies in place that prohibited using the information without authorization, or downloading it to a personal computer but did not restrict Miller’s ability to access the data.\textsuperscript{82} Miller ultimately resigned, but before resigning, his company alleged that their competitor instructed Miller to download confidential documents, and email them to his personal email account.\textsuperscript{83} After resigning, Miller gave a presentation, on behalf of the competitor, to a potential customer, which ultimately led to the competitor being awarded two projects.\textsuperscript{84}

The Court adopted definitions of the terms “without authorization” and “exceeds authorized access” that apply when individuals either accesses a computer without permission, or obtain or alter information on a computer beyond that which they are authorized to access.\textsuperscript{85} This distinction is important as there are times when employees may alter information on computers that they have access to, only to further their employment duties, such as an employee downloading a file to work on it from home.\textsuperscript{86} While working from a personal

\textsuperscript{75} Id. at 861.
\textsuperscript{76} Id.
\textsuperscript{77} Id.
\textsuperscript{78} Nosal, 676 F.3d at 861.
\textsuperscript{79} Id. at 862.
\textsuperscript{80} WEC Carolina Energy Solutions LLC v. Miller, 687 F.3d 199, 201 (4th. Cir. 2012).
\textsuperscript{81} Id. at 202.
\textsuperscript{82} Id.
\textsuperscript{83} Id.
\textsuperscript{84} Id.
\textsuperscript{85} Id. at 206.
\textsuperscript{86} Miller, 687 F.3d at 206.
computer may be against a company use policy, it would not be a criminal
offense punishable under the CFAA. 87 In this scenario, a company may
terminate an employee’s computer access, or administer any other punishment
in-house, but would not pursue criminal charges for such a breach of computer
use policies. 88 While Miller did download the files for personal use, which did
violate the company’s computer use policies, he could have downloaded them for
any reason, and simply because he used them to aid a competitor does not make
him liable under the CFAA. 89

Finally the Second Circuit also adopted a narrow approach to interpreting the
CFAA with United States v. Valle. 90 This case involves a set of disturbing facts
involving an individual, Gilberto Valle, who was an officer in the New York
Police Department. 91 While no evidence exists that Valle ever acted violently
towards anyone, he was a member of an active Internet sex fetish community. 92
In this community, Valle spoke with other members in depth about committing
atrocious acts of sexual violence. 93 While all this took place in fantasy based
chats with individuals that Valle may have never learned the identity of, Valle
did use images of women he knew, and sent them to other users describing
violent acts against them. 94 However, Valle was charged under the CFAA
because he used his access as a police officer to databases meant for police
officers, in order to obtain information on women he had discussed kidnapping
with one of the other members of this community. 95 Valle was aware at the time
that using the database for private use was a violation of Department rules. 96

Valle conceded that he violated the Department rules when he accessed the
database, but argued that he did not violate the CFAA because he was entitled to
obtain the information as part of his position. 97 Like the Ninth Circuit and Fourth
Circuit, the Court found that a broader interpretation would only affect a large
number of ordinary individuals. 98 Even though Valle accessed a government
computer, the CFAA affects all protected computers, which are essentially all
computers with internet access, and thus, a decision finding for a use policy
would affect the population as a whole. 99 Despite the uncomfortable
circumstances of this case, the Court did not find that Valle exceeded authorized

87. Id.
88. Id.
89. Id. at 207.
90. United States v. Valle, 807 F.3d 508 (2d Cir. 2015).
91. Id. at 512.
92. Id.
93. Id.
94. Id.
95. Id. at 513.
96. Valle, 807 F.3d at 513.
97. Id. at 523.
98. Id. at 527.
99. Id. at 508.
access.100 Echoing the concerns of the Ninth Circuit, the Court did not want to allow checking Facebook at work to become criminal, even though the prosecutor promised that minor violations would not be pursued.101

C. Broad Interpretation of the CFAA

The First Circuit Court was the first to find that a violation of a use restriction violated the CFAA.102 In EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577 (1st Cir. 2001), Explorica, Inc. was formed to provide global tours to high school students.103 Some employees of Explorica were previously employed by EF Cultural Tours BV, EF Institute for Cultural Exchange, Inc., EF Cultural Services BV, and Go Ahead Vacations, Inc. (collectively “EF”), which was the world’s largest private student travel organization.104 In order to be competitive, Explorica’s Internet consultant designed a “scraper” to obtain price and travel information from EF’s website.105 A scraper is a tool that is used on the Internet to pull data from websites by submitting multiple queries to it.106

The use of the scraper in this case allowed for Explorica to obtain information about their competitor without having to manually sort through the data.107 The scraper accessed the data twice, querying EF servers around 30,000 times each time.108 EF argued that a violation had occurred under the CFAA as Explorica had “knowingly and with intent to defraud” accessed their servers in obtaining this data.109 As some of the employees of Explorica were former employees of EF, plaintiffs contended that private information was used in order to create the scraper.110 Since the former employees of EF had signed broad confidentiality agreements, and specific company knowledge was used in order to create the scraper, it was likely that Explorica had violated the CFAA.111 In this respect the employee did not obtain the information before leaving the company, but used knowledge of how the company operated, and designed a tool using that knowledge.112 The CFAA also required that EF demonstrate damage or loss, and while damage was not provable, loss was shown as EF suffered a detriment and disadvantage by having to assess any possible damages caused by the scraper.113

100. Id. at 528.
101. Id.
102. Pyne, supra note 16.
103. EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 579 (1st Cir. 2001).
104. Id.
105. Id.
106. Id. at 579.
107. Id.
108. Id. at 580.
109. Explorica, 274 F.3d at 581.
110. Id. at 582.
111. Id. at 583-84.
112. Id. at 583.
113. Id. at 585.
In finding a violation of the CFAA, the Court focused on the fact that former employees voluntarily entered into a broad confidentiality agreement. Former employees exceeded authorization by using proprietary information in order to create the scraper. The information used in this case was not specific; it was merely “know-how.” In a stark contrast to the narrow opinions discussed above, this Court applied a broad interpretation of the CFAA to a broad interpretation of the confidentiality agreement.

The Fifth Circuit has held that violating restrictions against using customer’s personal information to incur fraudulent credit card charges is a violation of the CFAA. Dimetriace Eva-Lavon John was employed by Citigroup and had access to their database and customer information. John provided her half-brother with customer information that allowed him and others to create fraudulent charges. John argued that she was authorized to use her company’s computers and view records in the course of her normal duties. It was a company policy that employees were not able to use the information to perpetrate a fraud, make changes without a customer’s requests, nor remove material from the office building. The Court held that exceeding authorized access might include exceeding the purposes for which access is authorized, as John did, because she had access to records, but did not have authorized access to remove the records. The key difference between this interpretation and the Ninth Circuit’s is that when an individual has reason to know that they are not authorized to access data for a specific purpose, and are accessing that data with the intent to conduct a criminal scheme, then that conduct would be considered to exceed authorized access.

The Seventh Circuit held that when an employee engaged in misconduct that violated his employment contract, he terminated his employment relationship, and while he retained the physical ability to access the company database, the termination made any use of the database exceed his authorized access. Jacob Citrin was an employee for International Airport Centers, LLC (“IAC”), and was

---

114. Id. at 584.
115. Explorica, 274 F.3d at 583.
116. Id.
117. See Id at 583-85.
118. Pyne, supra note 16.
119. United States v. John, 597 F.3d 263, 272 (5th Cir. 2010).
120. Id.
121. Id.
122. Id. at 270.
123. Id. at 272.
124. Id. at 273.
provided a laptop that he recorded data on as part of his duties. Citrin wanted to quit and go into business on his own, and breached his employment contract. But, before Citrin returned the company laptop to IAC, he deleted all data in it, including data he had collected, and data that would have revealed his improper conduct prior to quitting. In order to make sure the deleted files were unrecoverable, Citrin used a program that was designed to write over the deleted files. The court found that using a program that had the specific purpose to permanently delete files would be considered a transmission under the CFAA. Citrin argued that he did not exceed his authorization as he was authorized to use the laptop.

To exceed authorized access, Citrin would have had to have his authorization to use the laptop revoked. By breaching his employment contract and his duty of loyalty, Citrin terminated his agency relationship with IAC. In terminating this relationship, Citrin no longer had any rights as an IAC employee and thus, had no authority to access the laptop. Citrin argued that his employment agreement authorized him to return or destroy data on the laptop at the cessation of employment. Citrin’s reliance on this provision was misplaced, as it was limited to confidential information, with the purpose of prohibiting the dissemination of confidential information. Therefore, Citrin’s action of deleting all the files on the laptop was a violation under the CFAA, as at that point in time, he had no authority to access the laptop.

Finally, the Eleventh Circuit adopted a broad interpretation of the CFAA and found that an individual using the social security administration database to get personal information on potential romantic partners was a violation. Roberto Rodriguez worked as a representative for the Social Security Administration and had access to databases that contained personal information such as social security numbers, addresses, dates of birth, and so on. The Social Security Administration had a policy that forbade employees from obtaining any of the information on the database for nonbusiness reasons. These policies were told to employees through training sessions, notices in the office, notices on their

127. Id.
128. Id.
129. Id.
130. Id.
131. Id. at 420.
132. Id. at 420.
133. Citrin, 440 F.3d at 420.
134. Id.
135. Id.
136. Id. at 421.
137. Id.
138. Pyne, supra note 16.
139. United States v. Rodriguez, 628 F.3d 1258, 1260 (11th Cir. 2010).
140. Id.
computers, and it was required that employees sign acknowledgment forms annually.\textsuperscript{141} Even though the Social Security Administration warned that the employees might face criminal penalties for violating the policies, Rodriguez refused to sign the forms for several years.\textsuperscript{142} The Social Security Administration gave employees unique identification numbers and eventually flagged Rodriguez’s number for suspicious activity, noting that he had accessed the personal records of 17 different people for nonbusiness reasons.\textsuperscript{143}

Rodriguez argued that he was authorized to use the databases and thus did not exceed authorized access.\textsuperscript{144} However, the government argued that violating the policy, and accessing information for nonbusiness reasons is exceeding authorized access.\textsuperscript{145} Rodriguez was found to have violated the CFAA for a few reasons.\textsuperscript{146} The first is the fact that the Social Security Administration told him that he was not allowed to use the system of nonbusiness reasons, and because of the extensive measures that the Social Security Administration used in order to convey this fact to their employees.\textsuperscript{147} Next, the purpose of Rodriguez’s actions was not called into question as the Court held that he exceeded authorized access by simply obtaining the personal information for a nonbusiness reason.\textsuperscript{148} Finally, Rodriguez may not have defrauded anyone or gained financially, but those factors are irrelevant when considering the misdemeanor penalty of the CFAA.\textsuperscript{149} Simply by accessing the information for a nonbusiness reason and thus, violating the use policy, Rodriguez was found to exceed authorized access.\textsuperscript{150}

III. PURPOSEFULLY VIOLATING TOs TO RESEARCH

As discussed above, the interpretation of the CFAA regarding ToS and computer use policies is varied throughout the circuits. Some of the courts that have interpreted the statute more narrowly have expressed the possibility of the government pursuing minor violations with the full force of the CFAA. This has created a fear among “white-hat” security testers and their possible liability under the CFAA.\textsuperscript{151} A white-hat security tester may also be known as a white-hat hacker.\textsuperscript{152} These white-hat hackers are specialist who purposefully breaks

\begin{thebibliography}{99}
\bibitem{141} Id.
\bibitem{142} Id.
\bibitem{143} Id.
\bibitem{144} Id. at 1263.
\bibitem{145} Rodriguez, 628 F.3d at 1263.
\bibitem{146} Id. at 1263-64.
\bibitem{147} Id. at 1263.
\bibitem{148} Id.
\bibitem{149} Id. at 1264.
\bibitem{150} Id.
\end{thebibliography}
security measures in order to test protected computers and networks so that vulnerabilities can be found prior to any malicious hacker, or black-hat hacker, finding them.\textsuperscript{153}

There are a numerous reasons why white-hat security testing is useful to consumers as a whole, yet some manufacturers do not support this idea as it will increase the amount of time and resources spent on a particular system.\textsuperscript{154} Whatever the reason may be, if a company is unable to assess all potential vulnerabilities, then its vulnerable nature may offer incentives to these white-hat hackers for such vulnerabilities will be found.\textsuperscript{155} This type of research identifies many issues before they become a threat.\textsuperscript{156} For example, researchers have found security flaws in medical devices like insulin pumps and pacemakers.\textsuperscript{157} These devices utilize the Internet to send data to health care providers, and in some instances can be controlled over the Internet as well.\textsuperscript{158} In 2007, the wireless function of Vice President Dick Cheney’s pacemaker was disabled as a precaution.\textsuperscript{159} A large problem with this is that these devices do not receive regular security updates in the same way personal computers, phones, and other devices do.\textsuperscript{160} For example, exposing flaws that potential hackers could have used to fix votes has helped make election processes more secure.\textsuperscript{161} As briefly mentioned before, vehicles have been tested to find vulnerabilities in cars that would have made them potentially susceptible to attacks.\textsuperscript{162} Finally, this type of research has been used to protect privacy on the Internet by studying how certain websites track activities online.\textsuperscript{163}

This last point deals not with the security of a website or of a device, but personal security. Companies use tracking systems in order to analyze individuals Internet behavior.\textsuperscript{164} As this data is collected and shared between websites, many people worry about the implication of a lack of privacy in the digital world.\textsuperscript{165} Privacy online is an important issue when considering that more

\begin{itemize}
\item \textsuperscript{153} Id.
\item \textsuperscript{154} The Computer Fraud and Abuse Act Hampers Security Research, supra note 151.
\item \textsuperscript{156} The Computer Fraud and Abuse Act Hampers Security Research, supra note 151.
\item \textsuperscript{157} Id.
\item \textsuperscript{158} Daniel Clery, Could a Wireless Pacemaker Let Hackers Take Control of Your Heart?, SCIENCE, (Feb. 9, 2015, 3:00AM), http://www.sciencemag.org/news/2015/02/could-wireless-pacemaker-let-hackers-take-control-your-heart.
\item \textsuperscript{159} Id.
\item \textsuperscript{160} Id.
\item \textsuperscript{161} The Computer Fraud and Abuse Act Hampers Security Research, supra note 151.
\item \textsuperscript{162} Id.
\item \textsuperscript{163} Id.
\item \textsuperscript{165} Id.
\end{itemize}
transactions are occurring online, transactions such as housing, credit, and employment.166 Recently, the ACLU, along with several researchers, filed a lawsuit claiming that the CFAA was unconstitutional.167 These researchers are unable to investigate companies’ online practices for fear of violating the ToS of particular websites, and thus, violating the CFAA.168 Professors Sandvig and Karahalios are attempting to determine whether real estate websites use computer programs that discriminate based on users race or other factors.169 Professors Wilson and Mislove are studying whether online hiring websites utilize discriminatory practices in a similar way.170 Through the ACLU, these professors and others filed a complaint to challenge the CFAA.171

The complaint alleged that data brokers compile information and sell this information for marketing purposes.172 This information is used and additional information, such as race, age, gender, religion, and ethnicity can be appended to consumers’ profiles, which follow individuals online.173 Additionally, the complaint alleged that this discrimination existed in past hiring decisions, as well as discrimination based on credit score and zip codes.174 Courts and Congress support audit testing as it has historically been a crucial way to discover racial discrimination in the housing and employment fields.175 Scraping, as discussed previously, is a common prohibition in a website’s ToS.176 Professors Sandvig and Karahalios create scrapers in their research, which mimic real people browsing the Internet.177 The professors would then use these fake people and have them represent individuals of different cultures in their Internet habits.178 After collecting enough browsing data, the fake individuals would then visit real estate websites and scrape the listings for data collection, which the professors would analyze to test whether discrimination occurred over the Internet.179 Other researchers would use similar techniques – creating fictitious accounts and

168. Id.
169. Spielman, supra note 166.
170. Id.
171. Id.
172. Id.
173. Id.
174. Id.
175. Id.
176. Id.
177. Id.
178. Id.
179. Id.
scraping the data – even though these techniques are against websites’ ToS, and the researchers were aware of this fact.180

One of the reasons the Ninth Circuit generally did not support computer-use policies that determined culpability under the CFAA was the implication that those polices, which can be amended or changed regularly, would dictate federal law.181 However, the other circuits are not clear on website ToS violations, and the circuits are split on computer-use policies, especially with regard to employers. But what about discrimination that occurs over protected computers at an employee’s workplace? What about harassment that occurs in the same way? Would an employer be able to insulate itself with a CFAA claim if all evidence of possible discrimination or harassment was on a protected computer?

IV. EMPLOYER AND EMPLOYEE RELATIONSHIPS AND CLAIMS UNDER THE CFAA

A. Discrimination and Harassment in the Workplace

A whistleblower provides valuable information to the government by reporting the wrongdoings of a company.182 To follow up on these allegations, the government will need documentation, or other evidence that will support the claims of wrongdoing.183 On the topic of whistleblowing to report discrimination or harassment, Human Resource personnel would advise the victim to keep personal documentation of each event.184 But how does one collect documentation, which can include emails, if those documents and emails are protected by company computer-use policy?185

Of course protections exist for individuals who disclose company documents, which are protected by confidentiality agreements, to organizations such as the Internal Revenue Service or U.S. Securities and Exchange commission.186 But for documents that don’t fall under one of these retaliation provision protections, the CFAA may be applicable because it covers a broader set of documents—those that aren’t even trade secrets.187 If a company has a computer-use policy

180. Id.
181. See generally United States v. Drew, 259 F.R.D. 449, 466 (C.D. Cal. 2009) (the opinion brings up the issue that if terms of service alone could be considered exceeding authorized access, then private companies would be defining when a federal law is violated).
183. Id.
185. Id.
186. Marshall & Schroeder, supra note 182.
187. Aravind Swaminathan & Marc Shapiro, “Don’t Go There”: Second Circuit Makes it Harder to Bring Claims against Former Employees who Take Company Information without
that prevents an employee from downloading work emails or forwarding them to a personal email account, what happens if employees receive emails that contain harassing or discriminatory evidence, and they forward it to their personal email address to save it? Alternatively, if a company has a policy against harassment, and an employee sends a discriminatory or harassing email to a co-worker, violating the policy, can the employer pursue a CFAA claim against that employee?

Generally, a whistleblower may be accountable for revealing confidential information if the information is truly confidential, and if the employee disclosed the information unlawfully. As previously mentioned, the CFAA does not delineate between truly confidential materials, also known as trade secrets. While public policy may support the employee’s releasing the information, the risk remains on the employee. Courts generally will weigh the seriousness of a confidentiality breach against the public policy of that breach. The government may not want to prosecute employees who introduce legitimate evidence, but under the CFAA, the government could prosecute an employee for mere unauthorized access to computer systems.

Wendi Lee sued her former employer, PSMI, Inc. (“PSMI”) for pregnancy discrimination, and PSMI answered by claiming a violation under the CFAA. PSMI claimed that Lee violated the company’s computer-use policies through her excessive internet use, visiting personal websites such as Facebook, and sending personal emails through her personal email account. Ultimately, PSMI’s claim against Lee failed because the court found the violation of company policy inapplicable. Some would claim that making the CFAA claim against an employee in this scenario is a form of intimidation. In this case, the court adopted the position of the Ninth Circuit and could not find that Lee’s use

---

189. Swaminathan & Shapiro, supra note 187.
190. Patrick, supra note 188.
191. See generally Quinlan v. Curtiss-Wright Corp., 204 N.J. 239 (N.J. 2010) (a case where an employee breached her confidentiality agreement with her employer, but to gather information for her claim).
194. Id. at *2.
195. Id. at *6.
of the computer was without authorization.\textsuperscript{197} Employers may not retaliate against individuals for filing charges of discrimination,\textsuperscript{198} but it is not clear whether filing a counterclaim alleging CFAA violations is retaliation.

In another case, Nicole Clarke-Smith worked as the Director of Human Resources for Business Partners in Healthcare, L.L.C. ("BPIH").\textsuperscript{199} Clarke-Smith and other employees felt discriminated against on the bases of race and sexual orientation.\textsuperscript{200} While Clarke-Smith was on a leave of absence, the U.S. Department of Labor investigated BPIH for problems with COBRA notices to former employees.\textsuperscript{201} BPIH believed Clarke-Smith knew of the investigation before her leave and concealed it from her supervisors.\textsuperscript{202} For this alleged concealment, and for failure to make timely 401(k) deposits, BPIH terminated Clarke-Smith.\textsuperscript{203}

Clarke-Smith filed a lawsuit in federal court, asserting claims under the Civil Rights Act of 1964.\textsuperscript{204} BPIH counterclaimed, asserting that Clarke-Smith violated the CFAA.\textsuperscript{205} BPIH argued that Clarke-Smith’s continued possession of her work-provided laptop after she was fired constituted unauthorized access.\textsuperscript{206} However, the court found that possession alone was not enough to count as access under the statute. Even if it were, the court reasoned, there was no evidence that Clarke-Smith accessed a protected computer after BPIH fired her.\textsuperscript{207} Because BPIH never proved access to a computer, the court did not have to address the issue of exceeding authorized access.

\textbf{B. Employment Issues Labeled as Hacking}

In the Ninth Circuit, an employee, Michael Weingand, filed a suit against his previous employer, Harland Financial Solutions, Inc. ("Harland") for wrongful termination and employment retaliation. Harland counterclaimed for, among other things, violations of the CFAA.\textsuperscript{208} Harland contended that Weingand sought personal files on his computer after termination and then obtained additional, unauthorized files.\textsuperscript{209} Ultimately, the court granted the motion

\textsuperscript{197} Lee, 2011 U.S. Dist. LEXIS 52828, at *6-8.
\textsuperscript{200} Id.
\textsuperscript{201} Id.
\textsuperscript{202} Id.
\textsuperscript{203} Id.
\textsuperscript{204} Id. at *3.
\textsuperscript{205} Clarke-Smith, 2016 WL 279094, at *3.
\textsuperscript{206} Id. at *10.
\textsuperscript{207} Id.
\textsuperscript{209} Id. at *5-6.
allowing Harland to pursue a claim under the CFAA. Harland pursued other claims against Weingand which is evidence that employers have adequate remedies available to them, and do not need to pursue claims under the CFAA. Interestingly, the Court allowed Harland to pursue its CFAA claim when the access restriction was merely a verbal restriction.

Conversely, there may be future instances of employees using the CFAA against their employers in a similar manner. If employers allow employees to use their own personal devices for work purposes, then the employees will have both work materials and personal materials on their devices. Upon termination, the employer would wipe the device of all data, including any personal data that may remain on the device, in an effort to delete any proprietary information. This would be the converse of Jacob Citrin’s case where the employee wiped the employer’s laptop. Seemingly this does indicate that an employee may have a valid claim against an employer that allows employee-use of personal devices for work purposes.

There are other possible issues that employers may worry about as well. For instance, an ex-employee brought a CFAA claim against an employer over the ownership of a LinkedIn account. The employer had a policy that after an employee left the company, the company owned the account and could use the information and see incoming traffic on it. The court found in favor of the employer on the CFAA claim because the employee did not allege any compensable damages. The ex-employee alleged that potential business opportunities and goodwill were lost, which are not compensable under the

210.  Id. at *20.
214.  See id.
215.  See id.
216.  Citrin, 440 F.3d at 419.
217.  See Valiulis & Geslewitz, supra note 213.
219.  Id.
220.  Id.
As individuals and companies continue using social media, this case shows that those individuals and companies can use the CFAA for situations that have nothing to do with hacking.222

But the threat of an employer using the CFAA in a lawsuit against an employee remains more likely. The CFAA—once considered only an anti-hacking statute—is now used as a counterclaim against employees by employers in cases of wrongful discharge and discrimination.223 There are many benefits for the employer who considers pursuing a claim under the CFAA.224 The fact that it is a criminal statute strengthens the seriousness of the employer’s claim, while also warning any other employees who might challenge the employer.225 Moreover, the CFAA provides an avenue for the employer to enter federal court—even though it may lack diversity.226 Additionally, in certain cases, under the CFAA, the employer can pursue a claim that is similar to trade-secret theft, without having to prove theft or whether the information taken is actually a trade secret.227

V. CONCLUSION

Three decades ago, the Congress implemented the CFAA to combat the threat of hacking during the Internet’s infancy. Today, with most individuals constantly connected to the internet through their phones and other devices, the CFAA proves to be either an obstacle, or a tool used by those wanting to protect special interests. In preventing hacking, the CFAA also prevents researchers from properly analyzing the ever-changing technologic landscape. The statute also encourages manufacturers not to inspect their own vulnerabilities thoroughly because if another user were to simply stumble upon vulnerability, then that action could be a violation of the CFAA—and the manufacturer could then pursue a claim against the user. Also, the CFAA has prevented researchers from examining new methods of discrimination that may be occurring through simple internet usage. Finally, the CFAA has become a tool that an employer can use against current and previous employees, as well as a tool that an employee may use against their current and former employers.

Most of the CFAA amendments have failed to make it through Congress. However, even if these amendments were to pass, they may not be enough in the

221. Id.
222. Id.
225. Id.
226. Neider & Diedrich, supra note 17.
227. Rogers & Hartman, supra note 224.
long term. The CFAA needs to be revamped, and in doing so, the following questions must be answered: Should an anti-hacking statute have the power to discourage security research? Should an anti-hacking statute turn into a tool to threaten employees who wish to bring claims against their employer? Parties use the CFAA as a catch all, applying it to claims where nothing else will stick, disregarding the original purpose of the CFAA. Congress enacted the CFAA to combat hacking, and now Congress needs to update the CFAA in response to the changing technological advancements made in the last thirty years.