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

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

Please send all manuscripts to the address given above. No manuscript will be returned unless return is specifically requested by the author.

Please note that this issue was published during the Northern Kentucky Law Review’s transition from the 19th edition of the Bluebook to the 20th edition. In light of this change, articles in this issue are cited to one edition or the other, but each article is consistent throughout.
SALMON P. CHASE COLLEGE OF LAW

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

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

JENNY YOUNG
Registrar of the College of Law

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

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

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

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

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

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

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

FACULTY

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

DONNA S. BENNETT, A.B., M.A., M.S.L.S.
Professor of Library Services & Assistant Director for User Services

JOHN M. BICKERS, A.B., J.D., LL.M.
Assistant Professor of Law

ROGER D. BILLINGS, JR., A.B., J.D.
Professor of Law

SHARLENE BOLTZ, B.A., J.D.
Professor of Law

CAROL BREDENMeyer, A.B., M.S.L.S.
Professor of Law & Director of Faculty Services

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

HARRY “Hap” DURKIN, B.S.
Director of Development

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

NANCY L. FIRAK B.S., J.D., LL.M.
Professor of Law

CAROL FURNISH, B.A., M.L.S.
Professor of Law & Director of Library Services & Assistant Director for Instruction & Outreach

RICHARD GRAVES, B.A., J.D., LL.M., LL.M.
Assistant Professor of Legal Writing

CHRISTOPHER GULINELLO, B.A., J.D., LL.M.
Professor of Law & Director of The Lunsford Academy

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

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

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

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

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

JENNIFER JOLLY-RYAN, B.A., J.D.
Professor of Legal Writing

KENNETH D. KATKIN, A.B., J.D.
Professor of Law

DONALD K. KAZEE, B.A., M.A., J.D.
Associate Professor of Legal Writing

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

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

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

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

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

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

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

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

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

MATTHEW J. TORKSON, B.S., J.D.
Professor of Law

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

COORDINATOR FOR THE PRO BONO PROJECT

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

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

CARYL A. YENENBAARD, A.B., J.D.
Professor of Law
EMERITI FACULTY

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

ADJUNCT FACULTY

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

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

Articles

Robert W. Dibert .................................................................................................................. 1

The Internet of Things: Emerging Legal Issues for Businesses
Mauricio Paez and Mike La Marca .................................................................................. 29

Comments

Hidden Threat: The Dark Web Surrounding Cyber Security
A. Dominick Romeo .............................................................................................................. 73

Notes

Against the Wind: Have We Accepted Data Breach as an Inevitability?
Charles Rust ...................................................................................................................... 87

Protecting Consumers in a Cyber World—Why the Federal Trade Commission Has the Advantage
Katelyn A. Marshall .......................................................................................................... 105
UNITED STATES CYBERSECURITY ENFORCEMENT:
LEADING ROLES OF THE FEDERAL TRADE COMMISSION
AND STATE ATTORNEYS GENERAL

Robert W. Dibert*

I. INTRODUCTION

Who has the Right to Control Personal Information?1
Who Assumes the Risk of Injury when Control is Lost?2

United States authorities historically left the protection of personal information to the individual, whether through prohibitions of government action3 or recognition of private rights and remedies.4 “By one assessment,


1. See, e.g., KY. REV. STAT. ANN. § 365.720(4) (2015) (“'Personally identifiable information' means data capable of being associated with a particular customer through one (1) or more identifiers, including but not limited to a customer's name, address, telephone number, electronic mail address, fingerprints, photographs or computerized image, Social Security number, passport number, driver identification number, personal identification card number or code, date of birth, medical information, financial information, tax information, and disability information.”); KY. REV. STAT. ANN. § 365.732(1)(c) (2015) (“Personally identifiable information' means an individual’s first name or first initial and last name in combination with any one (1) or more of the following data elements, when the name or data element is not redacted: 1. Social Security number; 2. Driver’s license number; or 3. Account number or credit or debit card number, in combination with any required security code, access code, or password to permit access to an individual’s financial account.”); see generally, CAL. CIV. CODE § 1798.80(e) (2015) (noting that although Kentucky’s data security breach notification law does not contain an express exemption for previously published information, some other states do); Id. (“Personal information does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records...”).

2. SEC’YS ADVISORY COMM. ON AUTOMATED PERS. DATA SYS., RECORDS, COMPUTERS, AND THE RIGHTS OF CITIZENS: REPORT OF THE SECRETARY’S ADVISORY COMMITTEE ON AUTOMATED PERSONAL DATA SYSTEMS, U.S. DEP’T. OF HEALTH, EDUC. AND WELFARE 29–30 (July 1973) [hereinafter “HEW Report”] (“[T]he life of a small-town man, woman, or family is an open book compared to the more anonymous existence of urban dwellers. Yet the individual in a small town can retain his confidence because he can be more sure [sic] of retaining control. . . . He lives in a face-to-face world, in a social system where irresponsible behavior can be identified and called to account.”).

3. See, e.g., U.S. CONST. amend. IV (“[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause . . . ”).

4. See, e.g., Grigsby v. Breckinridge, 65 Ky. 480 (Ky. Ct. App. 1867) (“An author retains a qualified property in the contents of letters written by him to others, and he alone has the right to
American society, prior to the Civil War, ‘had a thorough and effective set of rules with which to protect individual and group privacy from the means of compulsory disclosure and physical surveillance known in that era.’ However, the emergence of the national economy has made it often impractical—if not impossible—for individuals themselves to protect their personal information. In particular, use of computers and computer networks for personal and business transactions:

has resulted in the creation of vast amounts of individually identifying personal information. Online users may voluntarily disclose personally identifying information. ... Information about online users is also collected, sometimes without the user’s knowledge or consent ... through technology that routinely tracks, traces and makes portraits of every interaction with the network. ... Technology like data-mining software and the practice of online profiling facilitate the use of online personal information for commercial purposes.

In the face of this threatened loss of control, agencies of the United States government began to recommend stronger privacy protections.

Safeguards for personal privacy ... would require adherence by record-keeping organizations to certain fundamental principles of fair information practice:

- There must be no personal-data record-keeping systems whose very existence is secret.
- There must be a way for an individual to find out what information about him is in a record and how it is used.
- There must be a way for an individual to prevent information about him obtained for one purpose from being used or made available for other purposes without his consent.

publish them for his own benefit; and therefore, and also because they reflected his emotions and sentiments, he has a right to enjoin the publication of them by the recipient or any other person.”); Id. (recognizing common law copyright and right of privacy); Gregory v. Bryan-Hunt Co., 174 S.W.2d 510, 512 (Ky. Ct. App. 1943) (“Prior to 1890 the adjudicated cases both in this country and in England, which might be said to have involved a right of privacy ... were founded on a supposed right of property, or a breach of trust or confidence, or the like.”).


6. HEW Report, supra note 2, at 30 (“The impersonal data system, and faceless users of the information it contains, tend to be accountable only in the formal sense of the word. In practice they are for the most part immune to whatever sanctions the individual can invoke.”).


8. HEW Report, supra note 2, at 41.
There must be a way for an individual to correct or amend a record of identifiable information about him.

Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take reasonable precautions to prevent misuse of the data.9

In succeeding years, the United States began to enact sector-specific legislation implementing privacy protections.10 However, in contrast to members of the European Union, the United States has not created an administrative or other agency with specific responsibility to enforce privacy protections.11 Instead, the Federal Trade Commission and State Attorneys General have become de facto privacy commissioners in the United States.12

II. PRIVACY ENFORCEMENT BY THE FEDERAL TRADE COMMISSION

The Federal Trade Commission ("FTC") was created in 1914 to protect consumers from anticompetitive, unfair, or deceptive acts or trade practices.

The Commission is hereby empowered and directed to prevent . . . unfair methods of competition in or affecting commerce and unfair or deceptive acts or practices in or affecting commerce.

. . .

The Commission shall have no authority . . . to declare unlawful an act or practice on the grounds that such act or practice is unfair unless the act or practice causes or is likely to cause substantial injury to consumers which [sic] is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition. In determining whether an act or practice is unfair, the Commission may consider established public policies as evidence to be considered with all other evidence. Such public policy

9. Id.
11. See Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Jan. 28, 1981, CETS No. 108 (creating European Data Protection Supervisor, the European Union’s privacy protection agency).
12. See Kashmir. Hill, Will The U.S. Have a Privacy Commissioner Soon?, FORBES (Nov. 12, 2010), available at http://www.forbes.com/sites/kashmirhill2010/11/12/will-the-u-s-have-a-privacy-commissioner-soon/#182b35c16b38 ("The problem in the U.S. now is that a patchwork of laws and federal agencies have their hands in the privacy pot. If the U.S. does create a sole privacy watchdog, it will be following in the footsteps of a host of other countries that have passed Privacy Acts and created Privacy Commissioners to oversee them.").
considerations may not serve as a primary basis for such determination.  

The FTC has both administrative and judicial remedies available to combat unfair or deceptive practices. The FTC has both administrative and judicial remedies available to combat unfair or deceptive practices. 13 “[M]ost consumer protection enforcement is now conducted directly in court under Section 13(b) rather than by means of administrative adjudication.”  

In approximately 1995, the FTC began studying privacy issues in electronic commerce and promoting industry self-regulation to identify and remedy threats to the privacy of consumers’ personal information. 15 At about the same time, Congress began to authorize FTC enforcement of privacy issues in specific areas. 17 Within a few years, the FTC began to bring enforcement actions against what it perceived to be deceptive trade practices in connection with online marketing and consumer transactions. 18  

As early as 2000, the FTC had concluded that industry self-regulation would not provide sufficient safeguards for consumer privacy in the internet era. 19 After conducting a series of enforcement actions based upon allegedly “deceptive” data  

16. See U.S. West, Inc. v. FCC, 182 F.3d 1224 (10th Cir. 1999) (establishing that the FCC order restricting use and disclosure of customer proprietary information by telecommunications carriers violated the free speech clause of the First Amendment and that one reason for the FTC to encourage industry self-regulation in the first instance may be constitutional limits on the government’s ability to restrain commercial speech).  
19. See FED. TRADE COMM’N, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE, A REPORT TO CONGRESS 35 (2000) (“The 2000 Survey data, however, demonstrate that industry efforts alone have not been sufficient. Because self-regulatory initiatives to date fall far short of broad-based implementation of self-regulatory programs, the Commission has concluded that such efforts alone cannot ensure that the online marketplace as a whole will follow the standards adopted by industry leaders.”).
security practices, the FTC “began pursuing ‘unfair’ practices in 2005[.]”

These actions seem to share a common thread, in that the FTC expects businesses to be proactive in protecting consumers’ personal information:

> In our interconnected and data-driven economy, businesses are collecting more personal information about their customers and other individuals than ever before. . . . Businesses that store, transmit, and use consumer information can, however, implement safeguards to reduce the likelihood of data breaches and help prevent sensitive consumer data from falling into the wrong hands.**

After 20 years of investigation and enforcement against “deceptive” online practices, and 10 years of activity against “unfair” practices:

> the FTC has brought more than 100 spam and spyware cases and over forty data security cases. When the Commission challenges practices related to privacy and/or data security, it usually obtains an administrative or federal court order prohibiting future violations of the law and requiring the defendants to abide by their promises to consumers. In some cases, the order requires a defendant to implement a compliance program and to undergo audits administered by an independent third party every two years.**

The Commission’s summary reveals its case-by-case approach to identifying unfair or deceptive practices in the field of data privacy and security. But it also shows a proactive, preventive attitude. Not only do the proceedings “usually” contain forward-looking injunctive relief in addition to cease-and-desist; they also contain requirements for new compliance programs and biennial, independent audits. These forward-looking remedies require respondents in FTC proceedings, and by extension the business community at large, to consider data privacy and security to be evolving works in progress.

---

22. Id. at *1.
24. Id. at 4.
25. Id. at 2–5.
26. Id. at 3.
27. Id. at 7–9.
The FTC also has published a guide of principles from its past data privacy and security enforcement activities.28 The FTC Guide outlines and annotates ten basic principles for proactive security of consumer information:

1. Start with security.
2. Control access to data sensibly.
3. Require secure passwords and authentication.
4. Store sensitive personal information securely and protect it during transmission.
5. Segment your network and monitor who’s trying to get in and out.
6. Secure remote access to your network.
7. Apply sound security practices when developing new products.
8. Make sure your service providers implement reasonable security measures.
9. Put procedures in place to keep your security current and address vulnerabilities that may arise.
10. Secure paper, physical media, and devices.29

In addition to the enforcement citations contained in the FTC Guide, four specific proceedings illustrate elements of the FTC’s evolving approach to consumer privacy and data security: U.S. v. PLS Fin. Svcs, Inc.;30 In the Matter of HTC America, Inc.;31 Federal Trade Comm’n v. Wyndham Worldwide Corp.;32 and In the Matter of LabMD, Inc.33 The PLS proceeding was anchored in the FTC’s express authority to regulate data security practices of “financial institutions” and businesses that make use of consumer credit reports.34 Both HTC America and Wyndham illustrate extensions of the FTC’s scrutiny to more complex technology products and customer security; while LabMD may be a high-water mark of the FTC’s pursuit of “unfair” data security practices.35

---

A. PLS Financial Services ("Dumpster-Diving")

In June 2005, the FTC’s Disposal Rule\(^36\) became effective as an interpretation of the Fair Credit Reporting Act.\(^37\) Recognizing the dual worlds of hard copy and electronic storage, the Rule addressed both:

reasonable measures for disposing of consumer report information could include establishing and complying with policies to: burn, pulverize, or shred papers containing consumer report information so that the information cannot be read or reconstructed; destroy or erase electronic files or media containing consumer report information so that the information cannot be read or reconstructed; or conduct due diligence and hire a document destruction contractor to dispose of material specifically identified as consumer report information consistent with the Rule.\(^38\)

In *U.S. v. PLS Fin. Servs., Inc.* the FTC alleged that PLS operated payday loan and other consumer financial services businesses in more than eight states, so the FTC deemed PLS to be a “financial institution.” The FTC therefore alleged violations of the Disposal Rule, the Gramm-Leach-Bliley Act,\(^39\) the Fair Credit Reporting Act,\(^40\) the FTC Privacy Rule,\(^41\) and the FTC Safeguards Rule.\(^42\) The FTC also alleged that PLS’ “consumer privacy notice stated, ‘We maintain physical electronic and procedural safeguards that comply with federal regulations to guard your nonpublic information.’”\(^43\)

During its investigation, the FTC allegedly found that “intact documents containing consumers’ personal information were found on multiple occasions in dumpsters near PLS Loan Stores and/or PLS Check Cashers, which were unsecured and easily accessible to the public.”\(^44\) Allegedly, PLS “frequently failed to ensure that its customers were provided with a privacy notice, and required by the Privacy Rule describing its information collection and sharing practices with respect to affiliated and non-affiliated third parties.”\(^45\) In resolving


\(^{38}\) Id.


\(^{41}\) Privacy of Consumer Financial Information Act, 16 C.F.R. § 313 (2015).


\(^{44}\) Id. at *6.

\(^{45}\) Id. at *6–7.
the matter, PLS admitted no liability, but agreed to pay a $101,500 civil penalty for the alleged violations.\textsuperscript{46}


So-called administrative, physical & technical safeguards long have been part of the regulatory scheme underlying the Health Insurance Portability and Accountability Act ("HIPAA").\textsuperscript{47} The FTC extended the reach of safeguards through joint enforcement with the Department for Health and Human Services,\textsuperscript{48} and then through the FTC’s own proceedings.

HTC manufactures tablets & smartphones using the Android, Windows Mobile, or Windows Phone operating systems.\textsuperscript{49} The FTC alleged that HTC represented to consumers that they should follow standard manufacturer security procedures and location permissions in order to protect the privacy and security of their data.\textsuperscript{50} The FTC deemed these instructions to be unfair or deceptive, because HTC products allegedly contained specific vulnerabilities:

- Pre-installed custom apps did not include an option to configure or remove them;

- A custom voice recorder provided automatic recording capability to any installed app;

- HTC apps could be used to transmit location information or text messages without user consent;

- HTC apps could be used to download other apps without user permission; and

- HTC diagnostic and customer-support apps did not implement encryption or other manufacturer-recommended security measures.

\textsuperscript{46} United States v. PLS Fin. Servs., Inc., No. 1:12-cv-8334, at 5 (N.D. Ill. 2012), where are these sources in Drive - https://www.ftc.gov/sites/default/files/documents/cases/2012/11/121107pspaydaystip.pdf. We need these somewhere, every FN refers to different filings or final orders and we need to be able to see which one – can’t find this one on WL.


\textsuperscript{50} Id. at 1–2.
to prevent customer information from being intercepted or copied
without consent.51

Taken together, the HTC “vulnerabilities” seemed to consist of features that,
in combination, could be used to control and communicate users’ personal
information without either giving advance notice of that capability, or providing
an opportunity to disable or remove that capability from the device.52

The FTC then alleged that these technical vulnerabilities resulted from the
following administrative deficiencies that, in sum, constituted unfair or deceptive
practices:

- HTC allegedly failed to implement an adequate program to assess
  the security of products that it shipped to consumers;
- HTC allegedly failed to implement adequate privacy and security
guidance or training for its engineering staff;
- HTC allegedly failed to conduct assessments, audits, reviews, or
tests to identify potential security vulnerabilities in its mobile
devices;
- HTC allegedly failed to follow well-known and commonly-
accepted secure programming practices, including secure practices
that were expressly described in the operating system’s guides for
manufacturers and developers, which would have ensured that the
applications only had access to users’ information with their
consent; and
- HTC allegedly failed to implement a process for receiving and
addressing security vulnerability reports from third-party
researchers, academics or other members of the public, thereby
delaying its opportunity to correct discovered vulnerabilities or
respond to reported incidents.53

Notably, the FTC allegations began—but did not stop—with claims that
HTC failed to follow specific written recommendations for the operating systems
of HTC devices.54 Instead, the FTC also faulted HTC for an alleged lack of
proactive, forward-looking procedures to detect and respond to data privacy and

51. Press Release, Fed. Trade Comm’n, HTC America Settles FTC Charges It Failed to Secure
Millions of Mobile Devices Shipped to Consumers (Feb. 28, 2013), available at
https://www.ftc.gov/news-events/press-releases/2013/02/htc-america-settles-ftc-charges-it-failed-
secure-millions-mobile.

52. Press Release, Fed. Trade Comm’n, FTC Approves Final Order Settling Charge Against
HTC America Inc. (July 2, 2013), available at https://www.ftc.gov/news-events/


54. Id.
security vulnerabilities or incidents.\textsuperscript{55} In response to the FTC’s allegations, HTC did not admit any liability. HTC did, however, agree to:

- Establish, implement and maintain a comprehensive security program to (1) address security risks . . . of new and existing covered devices, and (2) protect the security, confidentiality and integrity of covered information. . . . Such program, the content and implementation of which must be fully documented in writing, shall contain administrative, technical and physical safeguards appropriate to respondent’s size and complexity, the nature and scope of respondent’s activities, and the sensitivity of the covered device functionality or covered information.\textsuperscript{.}

- Obtain initial and biennial assessments and reports (“Assessments”). . . . The reporting period for the Assessments shall cover (1) the first one hundred eighty (180) days after service of the order for the initial Assessment, and (2) each two (2) year period thereafter for twenty (20) years after service of the order for the biennial Assessments; and

- Retain for three years all materials used in connection with all compliance or Assessment activities taken under the consent Agreement and Order.\textsuperscript{56}

The 20-year period for biennial audits or assessments has become a common feature of FTC consent proceedings. However, the audit requirement itself, combined with the separate three-year retention period for compliance materials, creates new issues for records retention and compliance managers subject to those proceedings.\textsuperscript{57}

C. Wyndham Worldwide (Retail Data Security Breach)

The FTC began its enforcement of data security practices in approximately 2002, and began to scrutinize “unfair” data security practices in approximately 2005.\textsuperscript{58} Wyndham Worldwide Corporation is a hotel, resort, and vacation


\textsuperscript{56} HTC Am.,155 F.T.C. 1617 (F.T.C. 2013).

\textsuperscript{57} Memorandum from Kelly C. Tshibaka, Acting Inspector Gen., to Edith Ramirez, Chairwoman of the Fed. Trade Comm’n (Oct. 14, 2014) available at https://www.ftc.gov/system/files/documents/reports/141014oig-mgmtchallenges/pdf (noting that the FTC described its own internal assessment and introduction of recordkeeping processes and procedures: “FTC plans to utilize an Enterprise Content Management System (ECMS) to maintain agency records in electronic format. . . . RFO is working with agency stakeholders to develop information governance for FTC records. This includes taxonomy, common vocabulary, access controls, and retention triggers.”).

\textsuperscript{58} Julie Brill, Fed. Trade Comm’n., Keynote Address Before the Center for Strategic and International Studies – Stepping into the Fray: The Role of Independent Agencies in Cybersecurity
ownership enterprise with approximately 110,000 properties located in more than 100 countries.\textsuperscript{59} After investigation, the FTC alleged that Wyndham had suffered two data security breaches and failed to take reasonable security safeguards to prevent a third breach. In this case, the FTC alleged that Wyndham unreasonably failed to:

- Use complex passwords and security measures that could defeat “brute force” attacks;
- Maintain adequate inventory of devices connected to Wyndham’s networks;
- Maintain adequate firewalls against internet or inter-system intrusions; and
- Encrypt consumers’ payment card information.\textsuperscript{60}

In denying Wyndham’s motion to dismiss, the District Court also noted that the FTC alleged that the defendants “represented, directly or indirectly, expressly or by implication, that they had implemented reasonable and appropriate security measures to protect personal information against unauthorized access - but . . . did not[.\textsuperscript{61}]} In this case, the FTC also alleged that Wyndham’s data security deficiencies and breach incidents had resulted in the compromise of more than 619,000 consumer payment card accounts, and payment card fraud allegedly exceeding $10.6 million.\textsuperscript{62}

Wyndham appealed the District Court’s denial of the motion to dismiss. Interestingly, on appeal the FTC did not advance the notion that Wyndham had misrepresented the degree of security that it provided for customers’ personal information.\textsuperscript{63} Instead, the appeal proceeded as a direct challenge to the FTC’s ability to deem data privacy and security practices as “unfair” to consumers.\textsuperscript{64} In August 2015, the Court of Appeals for the Third Circuit ruled in favor of the FTC.\textsuperscript{65} The Court of Appeals Opinion squarely held that “certainly after the second time Wyndham was hacked, it was on notice of the possibility that a court could find that its practices fail the cost-benefit analysis [of an FTC unfair or

\textsuperscript{61} Id. at 626.
\textsuperscript{62} Id. at 609.
\textsuperscript{63} FTC v. Wyndham Worldwide Corp., 799 F.3d 236 (3d Cir. 2015).
\textsuperscript{64} Id. at 239 (noting that the first issue presented by Wyndham on interlocutory appeal was “whether the FTC has authority to regulate cybersecurity under the unfairness prong of § 45(a).”).
\textsuperscript{65} Id. at 236.
deceptive practices claim].”  The Court also pointed to FTC administrative precedent that put Wyndham on notice that its data security practices might be deemed unfair or deceptive. Finally, the Third Circuit deferred to administrative expertise of the FTC including Staff publications: The 2007 “FTC . . . guidebook, Protecting Personal Information: A Guide for Business . . . describes a ‘checklist[]’ of practices that form a ‘sound data security plan.’ . . . [the] FTC’s expert views . . . could certainly have helped Wyndham determine in advance that its conduct might not survive the cost-benefit analysis.”

Following the Third Circuit decision, the FTC announced a settlement in which Wyndham would agree, for a period of twenty years, to implement continuing administrative, technical and physical safeguards to protect the security of consumer payment card information. The safeguards include:

A. Designation of an employee or employees to coordinate and be accountable for the information security program;

B. Identification of material internal and external risks to “Cardholder Data” that could result in the unauthorized disclosure, misuse, loss, alteration, destruction, or other compromise of such information, and assessment of the sufficiency of any safeguards in place to control these risks. At a minimum, this risk assessment should include consideration of risks in each area of relevant operation, including, but not limited to, (1) employee training and management, (2) information systems, including network and software design, information processing, storage, transmission, and disposal, (3) risks emanating from the Wyndham-branded Hotels, and (4) prevention, detection, and response to attacks, intrusions, or other systems failure;

C. Design and implementation of reasonable safeguards to control the risks identified through risk assessment (including any risks emanating from the Wyndham-branded Hotels), and regular testing or monitoring of the effectiveness of the safeguards’ key controls, systems, and procedures;

D. Development and use of reasonable steps to select and retain service providers capable of appropriately safeguarding Cardholder Data they receive from Hotels and Resorts and requiring such service providers by contract to implement and maintain appropriate safeguards for such information; and

---

66. Id. at 256.
68. Id. at 256–57.
E. Evaluation and adjustment of Hotels and Resorts’ information security program . . . in light of the results of the testing and monitoring . . . that Hotels and Resorts knows or has reason to know may have a material impact on the effectiveness of such information security program.\textsuperscript{70}

The Stipulated Order also requires annual (not biennial) assessments of Wyndham’s compliance with the data security standards, and a special assessment with 180 days following discovery of any data security breach that involves more than 10,000 unique payment card numbers.\textsuperscript{71} “[A]ll materials relied upon to prepare [each] Assessment” must be retained for at least three years.\textsuperscript{72} The Stipulated Order appears to follow FTC practice of defining data security safeguards in terms of industry standards, and requiring periodic independent assessment of the adequacy of those safeguards. Wyndham may extend the FTC’s oversight, however, in that the Assessment period for Wyndham was shortened to an annual process, with provisions for special assessment in the event of a large data security breach. Wyndham also includes express reference to responsibility for selection and performance of third-party service providers.

D. \textit{LabMD (Refining the Risk of Injury?)}

Section 45(n) of the FTC Act provides that:

\begin{quote}
The Commission shall have no authority ... to declare unlawful an act or practice on the grounds that such act or practice is unfair unless the act or practice causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.
\end{quote}

The FTC’s Complaint Counsel alleged in LabMD, Inc., that the installation of peer-to-peer file sharing software on a billing manager’s computer, plus the discovery of personally-identifiable patient information in possession of suspected identity thieves, constituted an unfair practice because of the risk of identity theft.\textsuperscript{73} Complaint Counsel also alleged that LabMD did not have a comprehensive written information security program, and it “did not use readily available measures to identify commonly known or reasonably foreseeable security risks and vulnerabilities on its networks.”\textsuperscript{74} The FTC claimed that

\begin{itemize}
\item \textsuperscript{71} Id. at 6–8.
\item \textsuperscript{72} Id. at 12.
\item \textsuperscript{73} LabMD, Inc., No. 9357, 2014 WL 253518, at *9 (F.T.C. Jan. 16, 2014).
\item \textsuperscript{74} Complaint. ¶ 10(b), at 3, LabMD, Inc., No. 9357 (F.T.C. Aug. 29, 2013), \textit{available at} https://www.ftc.gov/sites/default/files/documents/cases/2013/08/130829labmdpart3.pdf.
\end{itemize}
records of patients had been placed at risk, where records were found in the possession of the alleged identity thieves and a file containing approximately 9,300 patient records allegedly was available from a LabMD computer using peer-to-peer file-sharing software.  

In response to the FTC’s allegations, LabMD moved to dismiss the administrative proceeding for lack of jurisdiction. In January 2014, the Commission squarely held that “LabMD’s Motion to Dismiss . . . calls on the Commission to decide whether the FTC Act’s prohibition of ‘unfair . . . acts or practices’ applies to a company’s failure to implement reasonable and appropriate data security measures. We conclude that it does.” Beyond its conclusion that the FTC had general authority to enforce secure data practices, the Commission also found that “the FTC and the Department of Health and Human Services (HHS) have worked together to coordinate enforcement actions for violations that implicate both HIPAA and the FTC Act.” In January 2015, the Court of Appeals for the 11th Circuit dismissed LabMD’s attempt to appeal the Commission ruling before the conclusion of the administrative adjudication.

Defending against the merits of the FTC’s administrative action, LabMD contended that the FTC Complaint was based upon improper testimony, from witnesses who were motivated to try to boost their company’s data security consulting business. LabMD also filed an action against the security consulting firm and certain individuals, claiming defamation, fraud, interference with business relations, misrepresentation, conspiracy, and racketeering.

In an Initial Decision, the Administrative Law Judge (ALJ) dismissed the FTC’s charges. The ALJ found that the FTC’s Complaint had been based upon the security company’s representations that a file of patient records had been downloaded from LabMD using peer-to-peer file sharing software. However, the ALJ found credible the testimony of a former employee of the company that he had been instructed to falsify internet records to make it appear that the file had been downloaded from LabMD. Consequently, the ALJ found that “Complaint Counsel has failed to prove the first prong of the three-part test – that this alleged unreasonable conduct caused or is likely to cause substantial injury to consumers.”

The Initial Decision also addressed the second data security incident, in which forty LabMD “day sheets,” nine copied checks, and one money order,
were found in the California house of individuals unrelated to LabMD. The day sheets contained the personal information, names and apparent social security numbers of 600 individuals, dating from June 2007 to March 2009. Two individuals eventually pled nolo contendere to identity theft. LabMD demonstrated that its day sheets were created, but not saved, electronically. The ALJ concluded that the FTC failed to prove that the exposure of the Sacramento documents was causally connected to any failure of LabMD to reasonably protect data maintained on its computer network. The evidence, according to the Initial Decision, failed to show that the documents were maintained on or taken from the computer network. The ALJ also held that the FTC failed to prove that the exposure “caused, or is likely to cause, any consumer harm.” The FTC’s proof that approximately 100 of the social security numbers appeared to have been used by people with different names was excluded for lack of foundation as to authenticity and reliability.

The Initial Decision noted that in the seven years the case had been ongoing, no individual had come forward as a victim of identity theft related to either of the alleged data security incidents. Further:

In light of the inherently speculative nature of predicting “likely” harm, it is unsurprising that, historically, liability for unfair conduct has been imposed only upon proof of actual consumer harm. Indeed, the parties do not cite, and research does not reveal, any case where unfair conduct liability has been imposed without proof of actual harm, on the basis of predicted “likely” harm alone.

The ALJ pointedly distinguished the Third Circuit’s decision in Wyndham:

Finally, in Wyndham, 2015 U.S. App. LEXIS 14839, which is the only court case that has upheld the FTC’s authority to bring an unfair conduct claim based upon alleged unreasonable data security, the court, in denying the defendant’s motion to dismiss, noted, inter alia, that “[o]n three occasions in 2008 and 2009 hackers successfully accessed Wyndham’s computer systems . . . [and] stole personal and financial information for hundreds of thousands of consumers leading to over $10.6 million dollars in fraudulent charges.” Id. at **3.
… the parties have not cited, and research does not reveal, any case in which unfair conduct liability has been imposed without proof of actual, completed harm, based instead upon a finding of “significant risk” of harm.93

To impose liability for unfair conduct under Section 5(a) of the FTC Act, where there is no proof of actual injury to any consumer, based only on an unspecified and theoretical “risk” of a future data breach and identity theft injury, would require unacceptable speculation and would vitiate the statutory requirement of “likely” substantial consumer injury. At best, Complaint Counsel has proven the “possibility” of harm, but not any “probability” or likelihood of harm. Fundamental fairness dictates that demonstrating actual or likely substantial consumer injury under Section 5(n) requires proof of more than the hypothetical or theoretical harm that has been submitted by the government in this case.94

On November 24, 2015, Complaint Counsel filed a Notice of Appeal of the Initial Decision to the full Commission.95 LabMD filed a “Notice of Conditional Cross-Appeal” on December 1, 2015, asserting that it should be allowed to cross-appeal additional grounds to support dismissal of the FTC Complaint if the full Commission were to decide to reverse the Initial Decision on its stated grounds.96 The Initial Decision noted that the term “likely to cause substantial injury” is not defined in the Act.97 Citing dictionary and judicial precedent, the ALJ defined “likely” to mean, “that it is probable that something will occur.”98 In so doing, the Initial Decision rejected Complaint Counsel’s argument that “injury may be sufficiently substantial ... if it does a small harm to a large number of people, or if it raises a significant risk of concrete harm.”99 The ALJ found that “Congress considered but rejected this standard.”100

On December 22, Complaint Counsel filed its brief on appeal to the Commission (“Appeal Brief”)101; including arguments that:

---

94. Id. at *14.
97. Id. at *57.
98. Id.
99. Id. (citations omitted).
100. Id.
the agency is not required to prove actual identity theft in order to establish that “a practice ‘causes or is likely to cause substantial injury’ under Section 5(n) of the FTC Act,” 15 U.S.C. § 45(n).\textsuperscript{102}

the agency need not quantify a risk of consumer harm in order to establish that a practice “causes or is likely to cause substantial injury”\textsuperscript{103} and

the Initial Decision incorrectly relied upon the injury-in-fact requirement for Article III (private party) standing to require proof of actual injury under Section 5(n).\textsuperscript{104}

In February 2016, LabMD filed its Answering Brief,\textsuperscript{105} which argued in part that there “is no decision or binding precedent where a respondent was found to have violated Section 5(n) based only on allegations regarding possible risk of likely substantial harm.”\textsuperscript{106} LabMD also argued that the proceeding is unconstitutional, because the “FTC admits that it has not prescribed regulations or legislative rules under Section 5 establishing medical data security standards that have the force of law.”\textsuperscript{107} Further, “[t]he FTC offered no evidence that the LabMD medical data security practices as alleged in 2007-2008 or at any time are likely to reoccur or likely to cause any substantial injury.”\textsuperscript{108}

FTC Complaint Counsel’s Reply Brief was filed on February 23, 2016,\textsuperscript{109} and reiterated that “Section 5 sets out two alternative justifications for Commission action – where a practice currently causes a significant risk of concrete harm, or where a practice is likely to do so in the future.”\textsuperscript{110} Complaint

\textsuperscript{102} \textit{Id.} at *11.

\textsuperscript{103} \textit{Id.} at *19.

\textsuperscript{104} \textit{Id.} at *21–22.

\textsuperscript{105} \textit{LabMD, Inc., In the Matter of, } \textit{FED. TRADE COMM.}, https://www.ftc.gov/enforcement/cases-proceedings/102-3099/labmd-inc-matter (last updated Feb. 5, 2016) [hereinafter \textit{Case Files}]. LabMD filed its Corrected Answering Brief on February 5, 2016, and filed its Consolidated Corrected Answering Brief on February 29, 2016. \textit{Id.}


\textsuperscript{107} \textit{Id.}, at 14.

\textsuperscript{108} \textit{Id.}, at 34. LabMD aimed squarely at allegedly improper use of information from Tiversa Corp. and its Chief Executive Officer, Robert Boback, emphasizing the Administrative Law Judge’s finding that “‘evidence and testimony provided by Tiversa was entitled to no weight’ and that the ‘FTC may not use evidence or any of the fruits thereof that was/were wrongfully obtained.’” \textit{Id.}, at 6, 64.

\textsuperscript{109} \textit{Case Files, supra} note 105.

\textsuperscript{110} Complaint Counsel’s Reply Brief, LabMD, Inc., No. 9357, at 10 (F.T.C. Feb. 23, 2016), https://www.ftc.gov/system/files/documents/cases/labmd_complaint_counsels_reply_brief_to_respondents_answering_brief.pdf. Counsel expressly relied upon the Third Circuit decision in \textit{FTC v. Wyndham Worldwide Corp.}, 799 F.3d 236, 246 (3d Cir. 2015) (“[T]he FTC Act expressly contemplates the possibility that conduct can be unfair before actual injury occurs.”), and \textit{FTC v. Neovi, Inc.}, 604 F.3d 1150, 1157 (9th Cir. 2010) (“An act or practice can cause substantial injury
Counsel argued that “significant monetary and non-monetary risks associated with identity theft and medical identity theft have been well documented, a failure to protect the information used to commit such crimes unquestionably causes or is likely to cause substantial injury.”¹¹¹ Consequently, “Section 5 liability under these circumstances does not depend on the happenstance of whether a company is breached and whether a victimized consumer can trace an identity theft incident back to the breached company.”¹¹² In addition, “Complaint Counsel is not relying in this appeal, nor did it rely below, on any opinions predicated on Mr. Boback’s testimony . . . or a document produced by Tiversa[.]”¹¹³

The Commission heard Complaint Counsel’s appeal of the Initial Decision on March 8, 2016, during which LabMD presented a slideshow to emphasize improper conduct by Tiversa and Mr. Boback, according to a Staff Report of the Committee On Oversight And Government Reform of the United States House Of Representatives.¹¹⁴ By Rule, the Commission is to issue its decision on the appeal within 100 days of the oral argument.¹¹⁵

Through its enforcement actions, the FTC has attempted to develop a body of data privacy and security law that compels truth in advertising, and also imposes affirmative duties upon businesses to develop and maintain industry-standard data privacy and security practices as the internet landscape evolves. Beyond these case-by-case enforcement activities, the FTC also has begun to issue Staff guidance that is intended to develop sound and proactive practices for safeguarding consumers’ personal information.¹¹⁶

¹¹¹ Id., at 11-12.
¹¹² Id., at 13-14.
¹¹³ Id., at 14.
¹¹⁴ Id., at 25. Complaint Counsel argued that the lack of reliance, and lack of Commission involvement in alleged wrongdoing by Tiversa or Boback, removed any taint that LabMD asserted in the proceeding. Id., at 35: “because there is no evidence that Mr. Boback or Tiversa acted at the direction of or in conjunction with the Commission or its staff, the exclusionary rule is inapplicable here.” Further, “the government ‘can be held responsible for a private decision only when it has exercised coercive power or has provided such significant encouragement, either overt or covert, that the choice must in law be deemed to be that of the State.’” Id. (quoting Blum v. Yaretsky, 457 U.S. 991, 1004 (1982)).
¹¹⁵ 16 CFR § 3.52(b)(2) (“The Commission will issue its final decision pursuant to § 3.54 within 100 days after oral argument”)
III. FTC GUIDANCE: PRIVACY BY DESIGN

The FTC’s policy work and staff reports build upon principles first articulated in the HEW Report. It also reflects a push by current Commissioners to harmonize U.S. privacy practices with European data protection standards where feasible. For example, the FTC participated in a May 2013 Global Privacy Enforcement Network Internet Privacy Sweep that “entailed a trawling by participating authorities of a set number of websites/mobile apps in a coordinated effort to assess the privacy practices of organizations as outlined in the privacy policies on their websites or within their mobile applications.” The FTC also participates generally in the Global Privacy Enforcement Network.

FTC Commissioners have often spoken about convergence of United States and European privacy principles:

A comparison of the US regime to protect consumer privacy with the draft EU privacy regulation highlights both our convergence on many of the goals around modernizing our privacy regimes, and our divergence on some of the mechanisms we choose to get there. The EU draft regulation reflects our common ground on many key issues -- promoting privacy by design, protecting children’s privacy, enhancing data security, and providing consumers with appropriate access, correction and deletion rights.

More specifically, “companies should build in consumer privacy protections at every stage in developing their products. These protections include reasonable security for consumer data, limited collection and retention of such data, and reasonable procedures to promote data accuracy[.]” The concept of “Privacy By Design” originated in 1995 with the Information and Privacy Commissioner of Ontario, Canada. As interpreted by the FTC:


118. GLOBAL PRIVACY ENFORCEMENT NETWORK, https://www.privacyenforcement.net/ (last visited Apr. 8, 2016).
120. Ohlhausen, supra note 23, at 4-5.
121. INFORMATION AND PRIVACY COMMISSIONER ONT., https://www.ipc.on.ca (last visited Apr. 8, 2016).
Companies should promote consumer privacy throughout their organizations and at every stage of the development of their products and services;

Companies should incorporate substantive privacy protections into their practices, such as data security, reasonable collection limits, sound retention and disposal practices, and data accuracy; and

Companies should maintain comprehensive data management procedures throughout the life cycle of their products and services.122

In sum, FTC “enforcement efforts have established what some scholars call ‘the common law of privacy’ in the United States.”123 The trend in FTC enforcement seems calculated to compel businesses to limit their use and control of personal information, absent informed consent by affected consumers. Where that consent has not been obtained, FTC enforcement seems designed to force businesses to assume the risk of injury when they lose control of the information. To date, the most significant restriction upon that trend has been the definition of “injury” sufficient to justify FTC intervention. At the international level, the FTC is the most prominent voice seeking to harmonize United States privacy principles with those of other nations.124

IV. PRIVACY ENFORCEMENT BY STATE ATTORNEYS GENERAL

State-government privacy legislation parallels the development of federal law, to some extent. That is, state laws often contain similar patterns of enforcement: specific sectors, security standards, requirements for secure disposal of personal information, and data security breach notification. However, state laws can vary in details such as thresholds, timing, and manner of enforcement. So this paper considers only some example statutes and enforcement notes.

A. General Protection for Personal Information

In contrast to the federal government, approximately 12 states have enacted legal duties for the protection of personal information generally.125

123. Brill, supra note 119, at 3.
125. E.g., CAL. CIV. CODE § 1798.81.5 (businesses “shall implement and maintain reasonable security practices and procedures” to protect personal information of California residents); 201 MASS. REGS. CODE § 17.01, et seq. (“Every person that owns or licenses personal information about
B. Secure Disposal Laws

Approximately 30 states have enacted laws requiring the secure disposal of consumer’s personal information.126

Like the FTC, states have gone dumpster-diving to enforce secure-disposal laws. In 2007, the Kentucky Attorney General’s “Identity Theft Prevention Initiative” inspected dumpsters on the premises of 121 businesses in major metropolitan areas across the Commonwealth. Of that number, a total of 47 businesses were identified as having improperly discarded personal information of more than 2,000 customers. All of the incidents were resolved through consent orders with the Attorney General.127 The Texas Attorney General instituted proceedings against a pawnshop, retail chain and pharmacy chain, for dumping customer records including bank statements, credit applications, healthcare records, and active credit/debit card numbers.128

More rounds of diving may be on the horizon:

[The] Massachusetts Institute of Technology (MIT) . . . bought 158 used hard drives from eBay and other sources . . . [that] had originally belonged to a variety of businesses ranging from banks to law firms . . . only 12 of the 158 hard drives had had their data destroyed in a way that kept the data from being recovered. From the other 146 drives, they recovered thousands of credit card numbers, social security numbers, medical records, emails, and other sensitive information.129

a resident of [Massachusetts] shall develop, implement and maintain a comprehensive information security program”).

126. E.g., CAL. CIV. CODE §§ 1798.80, et seq. (businesses must take all reasonable steps, including shredding or erasing, to dispose of records containing customers’ personal information “when they are no longer to be retained”); IND. CODE. §§ 24-4.9.2, et seq. (“database owners” may not dispose of records containing personal information of Indiana residents without shredding, incinerating, mutilating, erasing, or otherwise rendering the information unusable); KY REV STAT. §§ 365.720, et seq. (businesses must take reasonable steps, including shredding or erasing, to dispose of records containing customers’ personal information when they are no longer to be retained); MASS. GEN. LAWS ch. 931, § 2 (persons must dispose of records containing personal information of Massachusetts residents by redacting, burning, pulverizing, shredding, or erasing in order to prevent reading or reconstruction of the personal information).

127. See also Indiana v. Beck, No. 49D10-1412-PL-41613 (Marion Sup. Ct. Jan. 2015) (consent judgment including payment of $12,000 to the Attorney General for dumping 60 boxes of patient records into a dumpster behind a church).


“[I]t is likely that many edge devices will be replaced on a regular basis. It is important to establish policies and procedures for the secure disposition of devices that have held sensitive information or key material that could provide access to sensitive information.”

C. Data Security Breach Notification Laws

Approximately 47 states and several U.S. territories have enacted laws requiring businesses to notify consumers, and in various circumstances the state Attorney General and others, if a breach of information system security has occurred.131

States have been active in the enforcement of data breach laws.132 Similarly, in 2014 the Beth Israel Deaconness Medical Center settled with the Commonwealth of Massachusetts for a $100,000 penalty, costs of investigation and educational funding, arising from the loss of an unencrypted laptop containing health and other personal information of more than 3,900


131. E.g., CAL. CIV. CODE §1798.82 (requiring notification of individuals of unauthorized access to unencrypted computer data containing personal information of California residents, including notice to the Attorney General if notification must be made to more than 500 California residents); IND. CODE § 24-4.9 (requiring notification of individuals of unauthorized acquisition of unencrypted or unredacted computerized data containing personal information of Indiana residents, including notice to the Attorney General if notification must be made to more than 1,000 Indiana residents); Ky Rev Stat. Ann. §§ 365.732, et seq. (requiring notification of individuals of unauthorized access to unencrypted computer data containing personal information of Kentucky residents, including notice to the Attorney General if notification must be made to more than 1,000 Kentucky residents); MASS. GEN. LAWS ch. 93H (requiring notification of individuals of unauthorized acquisition of unencrypted data, or encrypted data together with a requisite access process or key, containing personal information of Massachusetts residents, including notice to the Attorney General and other state agencies); OHIO REV. CODE § 1347.12, etc. (requiring notification of individuals of unauthorized access to unencrypted computer data containing personal information of Ohio residents, including notice to the Attorney General if notification must be made to more than 1,000 Ohio residents).

132. E.g., Indiana v. WellPoint, Inc., No. 49D06-1010-PL-47381 (Marion Sup. Ct. June 2011) ($100,000 payment to the Attorney General plus up to two years’ credit monitoring or other relief for affected consumers, for alleged disclosure of personal information on an insurance application website and failure to provide timely notice to the Attorney General).
individuals.\footnote{Press Release, Attorney Gen. Mass., Beth Israel Deacones Medical Center to pay $100,000 Over Data Breach Allegations (Nov. 21, 2014), available at, http://www.mass.gov/ago/news-and-updates/press-releases/2014/2014-11-21-beth-israel-data-breach.html.} Contributing to the penalty amount was the Center’s delay for about 90 days from discovery of the incident, before notifying the Attorney General.\footnote{See also Massachusetts v. Briar Group, LLC, Civ. No. 11-1185B (Mass. Sup. Ct. Mar. 28, 2011) (including $110,000 in penalties in a consent judgment for alleged failure to comply with PCI/DSS standards for credit card processing; failure to control password usage and access to information systems; failure to alert customers of a known data security breach; and failure to encrypt payment card information stored on its servers).}

\section*{D. Future State Enforcement}

In July 2015, the National Association of Attorneys General wrote to Congress in consideration of proposed national standards for data security breach notification:

\begin{quote}
our offices regularly investigate the causes of data breaches to determine whether data collectors experiencing breaches used reasonable data security practices and notified consumers of the breaches according to the requirements of our state laws.
\end{quote}

\ldots

States should also be able to maintain their ability to place requirements on data collectors that go beyond those required at the federal level.\footnote{For example, the Health Insurance Portability and Accountability Act ("HIPAA") specifically does not pre-empt more stringent state privacy laws. P.L. 104-191, § 264(c); Letter from the Nat’l Ass’n of Attorneys Gen. to Mitch McConnell, Senate Majority Leader; John Boehner, Speaker of the House; Harry Reid, Senate Minority Leader; and Nancy Pelosi, House Minority Leader (July 7, 2015) (on file with author).}

For example, Massachusetts may assert extra-territorial jurisdiction of its protection laws to protect its residents.\footnote{See Rodney S. Dowell, Data privacy part I: Complying with new regulations to keep confidential personal information protected, MASSBAR ASS’N (Feb. 2010), http://www.massbar.org/publications/lawyers-journal/2010/february/data-privacy-part-i-complying-with-new-regulations-to-keep-confidential-personal-information-protected ("[t]he statute and regulations are intended to protect the “personal information” of Massachusetts residents when used by any business (in any jurisdiction), including law offices"); See also, Kearney v. Salomon Smith Barney, Inc., 137 P.3d 914 (Cal. 2006) (holding California’s two-party consent law for recording telephone conversations to override Georgia’s one-party consent when Georgia-based financial consultants spoke with California residents, but limiting retroactive relief to injunction).}

States also are collaborating in the enforcement of common data privacy principles. For example, in January 2015 the attorneys general of Massachusetts, Arizona, Connecticut, Florida, Kentucky, Maryland, North Carolina, Ohio, and
Pennsylvania, concluded a settlement with Zappos.com, Inc. Following unauthorized access to a Zappos server that contained customer names, addresses, telephone numbers, the last four digits of credit card numbers, and login credentials, the company agreed to a financial settlement and additional non-monetary relief, and to:

- Provide the attorneys general with its current security policy regarding customer information;
- Provide the attorneys general copies of reports demonstrating compliance with the Payment Card Industry Data Security Standard for two years;
- Have a third party conduct an audit of its security of personal information, provide the audit report to the attorneys general, and address any identified deficiencies; and
- Provide annual training to employees regarding its security policies.\(^{138}\)

Multi-state attorney general investigations also have been undertaken in connection with the Target\(^ {139}\) and Home Depot\(^ {140}\) data security breaches.

V. (TODAY’S) CONCLUSIONS

In the United States, there is no clear demarcation to identify “who has the right to control personal information?” With declining face-to-face transactions\(^ {141}\) and the rise of automated information systems\(^ {142}\), even the word


\(^{138}\) Id.


\(^{142}\) See Alex Louwe Koilmans, et al., TRANSACTION PROCESSING: PAST, PRESENT, AND FUTURE 5 (IBM Corp. 2012) (in today’s world, where almost everything we do is backed up with computer automation, nearly all of these business transactions drive one or more corresponding activities in the information system. When you buy a book, the cashier enters the amount in the register, rings up a total, and collects your money. That activity might send a number of requests to an information system: to take that book out of the inventory database, approve your credit card...
“who” may be somewhat metaphysical. The FTC and state attorneys general may be adapting to the world of faceless transactions by requiring “reasonable” proactive security measures, based upon industry standards such as PCI/DSS or emerging guidance of the National Institute of Standards & Technology (NIST). As of this writing, the FTC also seems to consider certain preventive practices to be significant:

- penetration tests or other automated tools, such as intrusion detection systems (IDS) or file integrity monitoring (FIM), to identify commonly known or reasonably foreseeable security risks and vulnerabilities;
- technologically limit the computer user rights for employees indiscriminately to download and install programs like peer-to-peer file sharing software from the Internet;
- use automated tools to monitor computers with access to personal information for any improper downloads, or configure firewalls, such as implementing IP address filtering, to prevent communication with the network by an untrusted source;
- maintain and update operating systems and other devices to protect against known vulnerabilities;
- implement a written information security plan, to provide IT employees with a roadmap for identifying security risks and choosing which security measures were necessary to protect against those risks, including employee training in the information security plan;
- prevent anonymous logins to information systems containing personal information;
- provide employees with the tools or training to encrypt emails containing sensitive personal information;
- implement strong password policies for employees and other system users; and
- restrict employee access to only the personal information necessary for the employee to perform his or her job, and minimize the exchange, update the store ledger, capture your store-loyalty status, and credit the store clerk with the sale. Each of these activities can be thought of as an IT transaction. Or, all of them together can be thought of as a transaction. Or, some of these activities might be divided into smaller transactions. It all depends on how the application is written.)

amount of personal information collected and stored in business operations.\textsuperscript{144}

“Who assumes the risk of injury” also is unsettled. The Initial Decision in LabMD seems to reflect a deeply rooted notion that “historically, liability for unfair conduct has been imposed only upon proof of actual consumer harm. Indeed, the parties do not cite, and research does not reveal, any case where unfair conduct liability has been imposed without proof of actual harm, on the basis of predicted ‘likely’ harm alone.”\textsuperscript{145}

On the other hand, where consumers rely upon the security of a data transaction, and enter into it at least in part on that basis, then a breach of the security of that system deprives those consumers of at least that benefit of the bargain.\textsuperscript{146} Of course, a breach also may result in a later injury that cannot be remedied.\textsuperscript{147} Finally, consumers may not understand the distinction between a privacy/security policy, and substantive privacy/security protection.\textsuperscript{148}

In these circumstances, consumers may expect the provider of the policy who lost control of the security of the information to assume all risks of loss associated with the breach. But Article III of the United States Constitution limits the scope of loss that may be deemed a cognizable “injury” for purposes of private litigation and redress.\textsuperscript{149}

\textsuperscript{144} Appell Brief, \textit{supra} note 101, at 26–29.
\textsuperscript{146} See Appell Brief, \textit{supra} note 101, at 9 ("exposure need not result in further injury—the mere disclosure is the harm").
\textsuperscript{147} Id. at 25 ("data breach victims experienced identity fraud at rates seven to eleven times that of consumers who had not been notified they were involved in a data breach, constituting absolute rates of 11.8% to 30.5%, with the risk increasing year over year") (citation omitted).
\textsuperscript{148} See Joseph Turow, et al., \textit{The Federal Trade Commission and Consumer Privacy in the Coming Decade}, 3 ISJLP, 723 (2007–2008) ("When consumers see the term “privacy policy,” they believe that their personal information will be protected in specific ways. . . . Of course, this is not the case").
\textsuperscript{149} See Joseph Turow, et al., \textit{The Federal Trade Commission and Consumer Privacy in the Coming Decade}, 3 ISJLP, 723 (2007–2008) ("When consumers see the term “privacy policy,” they believe that their personal information will be protected in specific ways. . . . Of course, this is not the case").
The appeal of the Initial Decision in *LabMD*, and increasing activism by state attorneys general, therefore may clarify the extent to which regulatory authorities may prescribe and enforce data privacy and security practices without a specific statutory mandate, or tangible consumer injury.

necessarily synonymous with ‘tangible.’ Although tangible injuries are perhaps easier to recognize, we have confirmed in many of our previous cases that intangible injuries can nevertheless be concrete”) (citations omitted). “Congress may ‘elevat[e] to the status of legally cognizable injuries concrete, de facto injuries that were previously inadequate in law.’” Id. However, “deprivation of a procedural right without some concrete interest that is affected by the deprivation . . . is insufficient to create Article III standing[.]” Id., quoting Summers, 555 U.S. at 496. In *Spokeo*, the Ninth Circuit “did not address the question . . . whether the particular procedural violations alleged in this case entail a degree of risk sufficient to meet the concreteness requirement. We take no position as to whether the Ninth Circuit's ultimate conclusion—that Robins adequately alleged an injury in fact—was correct.” *Id.*, at *9.*
THE INTERNET OF THINGS: EMERGING LEGAL ISSUES FOR BUSINESSES

Mauricio Paez and Mike La Marca*

I. INTRODUCTION

The “Internet of Things,” or IoT, is widely heralded as a game-changing phenomenon that could fundamentally alter consumer habits and transform the way commercial enterprises do business. According to McKinsey Global Institute, the IoT has the potential to alter the way people live and work, and drive significant economic transformations.\(^1\) FTC Commissioner Maureen Ohlhausen likewise noted that, “[IoT] capabilities have the potential to revolutionize many fields, including manufacturing and logistics, medicine, transportation, and energy.”\(^2\) The economic impact of such a revolution could be staggering: a study by Cisco forecasts that the IoT will have an impact of over $14 trillion by 2022.\(^3\) Similarly, Goldman Sachs noted that the structural change that will result from the IoT will be analogous to the industrial revolution.\(^4\)

While the IoT is still in the nascent stage of development, businesses have taken notice. A 2013 survey by The Economist found that over 75% of companies were already leveraging IoT technology or actively exploring it, with the vast majority of business leaders indicating that the IoT will eventually have a meaningful impact on how their respective companies conduct business.\(^5\)

* Mauricio Paez is a Partner and Mike La Marca is an Associate in the New York office of Jones Day and are members of the firm’s Global Cybersecurity, Privacy & Data Protection Group. The Authors would like to thank Austin Kim, Associate at Jones Day, for assisting with the research and preparation for this work. The views expressed in this article are solely of the Authors, and not of Jones Day or its other Partners.

that same study, the majority of business leaders surveyed believed that companies would inevitably fall behind their competition if they were slow to integrate IoT technology into their business. As a result, many companies have begun addressing their shortage of IoT-related skills and knowledge through aggressive training and recruitment campaigns. IBM, for example, reportedly invested $3 billion to build a new IoT division, and has begun training more than 2,000 consultants, researchers, and developers. Governments are also ramping up investments in the IoT, with the Chinese government expected to invest more than $600 billion in the IoT through 2020.

While many businesses are beginning to leverage the IoT in an effort to increase revenue, improve operational efficiency, and obtain a competitive advantage, the adoption of IoT technology will also trigger innumerable legal issues, many of which are novel and uncertain. Data privacy and cybersecurity are frequently cited as posing the greatest legal challenges, but a broad range of additional legal issues will need to be accounted for, including intellectual property rights and products liability. These legal issues will overlap, complement, and oftentimes contradict one another. In particular, the globalized nature of digital technology and data flows means that a company’s IoT operations will necessarily implicate multiple jurisdictions’ legal regimes, most of which are incongruous, territorial, and in a constant state of fluctuation. Additionally, because the IoT ecosystem hinges on the interconnectivity of countless devices and participants, companies will need to account for the legal rights and obligations of multiple stakeholders involved throughout a product’s entire lifecycle, from design and manufacturing to installation, operation, maintenance and decommissioning.

The authors address the privacy and cybersecurity concerns of the IoT for U.S. businesses, and other unique and pressing legal issues that businesses should contemplate when engaging with IoT technology. These issues will have a profound impact on IoT development, as well as the potential commercial and societal value it can generate. The following sections provide an analysis of new and unsettled legal issues for businesses to consider when evaluating how, and to what extent, the IoT should be adopted and aligned with the overall goals of their organization.

6. Id. at 13.
II. THE “INTERNET OF THINGS:” A BACKGROUND

Despite the growing pervasiveness of the “Internet of Things” it is not a single, unified concept: there is no universally agreed-upon definition of the IoT. Broadly speaking, however, the IoT refers to the growing number of everyday physical objects or “things” that have been embedded with technology to enable them to interact with the physical environment, people, and other devices in real-time. While computers and mobile devices are generally not classified within the IoT, smartphones and tablets contain sensors and other IoT-related technology, and often serve as a wireless hub or remote control for other “connected” objects through mobile apps.

Three key steps underpin the IoT. First, embedded sensors in IoT objects detect and capture data from the surrounding environment, including the people who own and operate those objects. In general, the IoT’s myriad sensors can be expected to collect data about environmental conditions (e.g., location, weather), individuals’ physiological measurements (e.g., heart rate, stress), and machine operations (e.g., activity, functionality), among other things. Second, this data is transmitted over an Internet-connected network and often stored using cloud-based applications. Third, that data is then analyzed for insights and intelligence that will guide decision-making. This third, most important step—the analysis of massive troves of data—can, among other things, improve the productivity of current organizational processes, enable new and more customized types of products and services, decrease waste and increase efficiency, and advance safety and security.

In sum, the IoT marks a paradigmatic departure from the Internet technology of previous decades: instead of simply facilitating human interaction through machine-to-machine communications, the IoT allows devices to measure and interact with the physical environment, gather information from that environment, and transmit that information to other devices, people, or environments. In this new terrain, the IoT allows smart objects to interact and collaborate with each other, as users of the IoT network.

The IoT ecosystem is currently growing at a rapid pace. Already, IoT technology is implemented into myriad individual consumer objects, from wearable devices like mobile fitness trackers and clothes that monitor an infant’s temperature, to Internet-enabled home appliances like self-learning refrigerators and coffee brewers, to home-automation systems that provide a single platform for individuals to remotely control the lights, temperature, electronics, and just about everything else in their home. However, the IoT also extends well beyond everyday consumer products. Medical devices, such as connected insulin pumps, pacemakers, and pill-shaped cameras are facilitating more efficient and precise healthcare services. “Smart” technology, like high-tech cruise control, navigation, real-time diagnostics, and crash-avoidance systems are currently deployed in vehicles to increase safety and convenience. Google and other manufacturers are even hoping to end human error behind the wheel altogether with the development of the autonomous vehicle.14 Through sensors, utility companies are monitoring smart-meter energy usage in order to customize their service offerings, detect upcoming maintenance issues, and remotely maintain certain smart meters. Enterprises throughout different industries are also increasingly utilizing IoT logistics applications to automate and streamline their supply chain management processes.15

Despite this staggering growth, we are still only in the early stages of the IoT. This ecosystem will only continue to explode over the next decade: technological advancements have driven down the costs of sensors, processors and other IoT technology, while smartphones, wireless coverage, and massively scalable computing power are becoming increasingly available and ubiquitous.16 Between 2013 and 2020, the digital universe will grow by a factor of 10—from 4.4 trillion gigabytes to 44 trillion.17 To put this in perspective: in 2010, for the first time in history, the number of connected devices outnumbered the number of humans. By 2020, however, it is estimated that there will be 50 billion connected devices, approximately six devices per person on the planet.18

same year, the available storage capacity will be able to hold less than 15% of the
digital universe.19 Experts predict that the Internet will become “so effortlessly
interwoven into daily life that it will become invisible, flowing like electricity.”20

As IoT technology advances, so will its significance. For example,
individual self-driving cars may drive the development of “smart citywide
transportation systems that route cars, alleviating congestion, conserving energy
and reducing accidents.”21 Such advancements could also translate into dramatic
improvements and unprecedented growth in diverse markets like healthcare,
energy, transportation, logistics, and manufacturing.22 The impact in healthcare,
for example, is expected to range from $1.1 trillion to $2.5 trillion per year by
2025, most notably from improved efficiency in treating patients with chronic
conditions through use of sensors, like glucose sensors, for remote monitoring.23
In manufacturing, the use of sensors to track the status of machinery and monitor
the flow of inventory, while implementing real-time updates to reduce downtime,
is estimated to achieve gains of $900 billion to $2.3 trillion per year by 2025.24

Governments throughout the world, including the U.S. government, have
also begun looking deeply into the implications of the IoT. In November 2014,
the National Security Telecommunications Advisory Committee issued its Report
to the President on the Internet of Things.25 Notably, the report emphasized the
enormous cybersecurity implications of the IoT, warning that technology
advances were outpacing the development of IoT governance structures and
related policies at both the national and global level. Since then, the U.S.
Congress has devoted more attention to the growing IoT landscape. In March
2015, for example, the U.S. Senate passed a bipartisan resolution recommending
that Congress adopt a national strategy for incentivizing the development and
growth of IoT in the U.S.26 The U.S. House of Representatives referred a similar
resolution to the Subcommittee on Commerce, Manufacturing, and Trade.27

19. TURNER, supra note 17, at 3.
20. JANNA ANDERSON & LEE Raine, DIGITAL LIFE IN 2025, at 5 (Pew Research Ctr., 2014),
21. SANFORD REBACK & TONY COSTELLO, DECONSTRUCTING THE INTERNET OF THINGS 2
22. Id. at 1.
23. MANYIKA ET AL., supra note 1, at 54
24. INTERNET OF THINGS: PATENT LANDSCAPE ANALYSIS, supra note 11, at 2.
25. THE PRESIDENT’S NAT’L SEC. TELECOMM. ADVISORY COMM., NSTAC REPORT TO THE
President Obama’s administration also joined these calls for IoT growth, proposing to spend nearly $4 billion over the next ten years to accelerate the acceptance of driverless cars in the U.S.\(^28\)

The IoT revolution has already begun. It will transform many enterprises into digital businesses, facilitate entirely new business models, and generate additional forms of revenue streams.\(^29\) And while the IoT will provide greater efficiency (such as by automating tasks, exchanging information, performing updates, making adjustments, maintaining thresholds, and comparing variances),\(^30\) it will also bring new business and legal challenges.

III. PRELIMINARY ISSUE: INTEROPERABILITY

Unlike the Internet, which is one giant ecosystem, the 50 billion interconnected objects expected by 2025 could exist in millions of different ecosystems. The reason the IoT still lacks a single, agreed-upon definition is because its future is still far from certain. The overarching definition of the IoT offered above encompasses a broad spectrum of activity from the general to the highly specific: on one end of the spectrum, the IoT could amount to a grand vision of a global, immersive network of sensors, information transmitters, cameras, and other devices built into anything and everything, allowing them to communicate constantly and seamlessly to revolutionize how we interact with the world.\(^31\) Alternatively, it could refer to nothing more than a discrete Radio Frequency Identification (RFID) chip attached to our smart coffee mug to facilitate personalized ordering at our local coffee shop.\(^32\) In other words, the IoT can range from vast, open systems that can interface with anything, to a finite, closed network designed to accomplish a limited purpose.\(^33\)

One of the fundamental challenges to the future of the IoT market is whether the technology developed for one market will be able to interface horizontally with the platforms of other markets. Standardized technology is necessary to connect objects and process information from a variety of different sources, regardless of manufacturer, model, platform, or industry. The IoT may only


\(^{31}\) PAUL KOMINERS, INTEROPERABILITY CASE STUDY: INTERNET OF THINGS (IoT) 6 (The Berkman Ctr. for Internet & Soc’y at Harvard Univ., 2012), available at https://cyber.law.harvard.edu/node/97248.

\(^{32}\) Id.

\(^{33}\) Id.
reach its full economic potential if businesses cooperate and agree on common standards for platforms to communicate with each other across different devices, applications, and operating systems. One study found that interoperability among multiple IoT systems accounts for 40%—and thus trillions of dollars—of the total potential value that can be unlocked through use of the IoT, while the ability to integrate and analyze data from various IoT systems accounts for 60% of that value.\(^\text{34}\)

At the moment, however, firms are independently developing distinct IoT ecosystems that limit interaction only to products and devices within their brand’s product line.\(^\text{35}\) For example, an Internet-Protocol camera developed by one vendor may not be able to communicate or interact with a home automation system manufactured by another. This kind of vertical integration is becoming even more pronounced as large technology companies use their resources to corner markets with their proprietary solutions.\(^\text{36}\)

Firms are often economically incentivized to rely on their own unique proprietary standards or closed systems to protect their intellectual property and gain a competitive advantage in the market place. Vendors can lock-in users to their particular ecosystem by increasing the cost to consumers of changing brands or substituting components from a different manufacturer.\(^\text{37}\) Proponents of interoperability argue that such turf wars will, in the long-term, stifle innovation, diminish operational efficiencies, and inhibit consumer choice. Conversely, from a cost-benefit perspective, firms may feel that any long-term benefits achieved from designing interoperability features into a product are outweighed by short-term risks like increased costs, design trade-offs, or reduced product performance.\(^\text{38}\) Moreover, at this stage of the IoT’s evolution, there is also the risk that overly-prescriptive regulation regarding standardization may inhibit the emergence of better architecture via trial and error in the market.\(^\text{39}\)

Regardless of the business justifications, however, it is clear that this “walled-garden” approach could lead to market fragmentation rather than an open, horizontal IoT ecosystem. Even further, when core technological elements of the IoT architecture are patented, third-party users seeking to incorporate those fundamental components into their product’s design may be forced to either pay licensing fees or illegally infringe those patents. It is thus unclear how interoperability will emerge on the systemic level, or if it ever will.

---

34. Manyika et al., supra note 1, at 4.
37. Rose et al., supra note 35, at 31.
38. Id.
Several industry coalitions have thus dedicated themselves toward working with the IoT community to promote open source software frameworks and harmonize standards and protocols related to the IoT in order to facilitate collaborative development and device-to-device connectivity. As the Internet Society opines, however, the time and investment required by stakeholders to participate in these wide-ranging standardization efforts will likely be costly, undermining the willingness of key players to participate meaningfully. Further, with the myriad and often uncoordinated standardization efforts taking place, “there is likely to be overlap and even conflicting standardization strategies between some efforts.” The absence of coordination across efforts could result in conflicting protocols, delayed product deployment, and fragmentation across IoT products, services, and industry verticals.

Others groups, including key players in the smartphone industry, have focused on defining core technology as a “standard essential” and compelling owners of “standard essential patents” (SEPs) to offer non-exclusive licenses to third parties on fair, reasonable, and non-discriminatory (FRAND) terms. SEPs are patents that are essential to implement a particular industry standard as it is impossible to manufacture products that follow a specific standard without using the technology covered by an SEP. FRAND terms are typically formulated by standard setting organizations (SSOs) to facilitate the interoperability of products from different manufacturers and ensure that product innovation follows a predetermined path. Companies that agree to FRAND terms or free use of their SEP’s forfeit a large piece of a small pie in the hopes of growing the overall pie through market innovation and obtaining a sizeable share of that pie in the future.

40. The AllSeen Alliance, for example, is a cross-industry consortium that consists of over 200 member companies, including Microsoft and Qualcomm, and is dedicated to promotion IoT interoperability through an open source, universal software framework. See AllSeen Alliance, The AllSeen Alliance Mission, LINUX FOUND., https://allseenalliance.org/alliance/our-mission (last visited Apr. 9, 2016). Likewise, the Open Interconnection Consortium, an industry group created by Intel, Broadcom, and Samsung, seeks to “define a common communication framework based on industry standard technologies to wirelessly connect and intelligently manage the flow of information among devices, regardless of form factor, operating system or service provider.” OPEN CONNECTIVITY FOUND., http://openconnectivity.org (last visited Apr. 9, 2016). It sponsors the IoTivity Project, an open source software framework enabling seamless device-to-device connectivity. See id.

41. ROSE ET AL., supra note 35, at 33.

42. Id.

43. Id.


But even if FRAND terms are possible, interested parties often profoundly disagree on what constitutes “fair and reasonable” licensing fees. Additionally, while a grander-scale IoT with seamless interoperability across devices will revolutionize industries and may generate trillions in revenues, it also carries its own unique issues and burdens. For example, the privacy and cybersecurity risks of a limited, privately owned IoT system that does not accept unverified devices are obviously less pronounced than a larger system with more dispersed ownership. More generally, in an economy where massive data streams are transmitted and shared among devices from different manufacturers, who owns the data? Who determines how and to what extent the data is used? Where and how should the data be stored? Who is responsible when something goes wrong? Legal risks in diverse fields such as data privacy, cybersecurity, intellectual property and products liability will grow in magnitude as the scale of IoT interoperability expands. The eventual scope and breadth of the IoT will ultimately shape the issues entities face as well as their strategies for managing the concomitant legal risks.

IV. PRIVACY

Many of the traditional privacy risks inherent to Internet-based technology are simply amplified by the nature of the IoT. As the IoT evolves, the exponential increase of connected devices will enable the collection of unparalleled amounts of data. Much of the data processed by IoT systems, particularly those in business-to-business applications, will not include personally identifying information, and thus will not raise personal data privacy legal issues. On the other hand, the ubiquity of connected devices will intensify the volume and variety of personal data that can be exploited in unauthorized

---

46. See, e.g., C-170/13, Huawei Technologies Co. v. ZTE Corp., 2015 EUR-Lex CELEX LEXIS 477 (July 16, 2015), available at http://curia.europa.eu/juris/celex.jsf?celex=62013CJ0170&lang1=en&type=TXT&ancre=. This dispute between Huawei Technologies Co. Ltd. (“Huawei”) and ZTE Corp. (“ZTE”) arose out of Huawei’s patent on Long Term Evolution (“LTE”), an LTE technology that is essential to mobile phone manufacturing. Id. Huawei made a commitment to the European Telecommunications Standards Institute to grant licenses to third parties on fair, reasonable, and non-discriminatory (“FRAND”) terms. Id. ZTE’s products use this technology and ZTE sought out a licensing agreement from Huawei on FRAND terms. Id. However, Huawei and ZTE were unable to agree on terms that were fair and reasonable, and Huawei ultimately sought an injunction against ZTE before the Düsseldorf Regional Court in Germany. Id. ZTE claimed that the action for a prohibitory injunction was an abuse by Huawei of its dominant position in the marketplace, since ZTE was willing to negotiate a license. Id. The German court referred those questions to the European Court of Justice, which determined that the proprietor of an SEP that alleges infringement could not bring an action for a prohibitory injunction or for the recall of products against the alleged infringer without notice or prior consultation with the alleged infringer, even if the SEP was already in use by the alleged infringer. Id.

ways and by unauthorized individuals, raising concerns about the difficult if not impossible task of maintaining privacy in the IoT era. 48

More unique to the IoT is the concern that data collected from connected objects can lead to behavioral profiling by revealing sensitive patterns, habits, preferences, physical conditions and other information about a unique individual over time. 49 Similar to mobile apps, IoT devices are often highly personalized and collect information that a user would consider particularly private, like health information or data on an individual’s location and movements. 50 A smart meter that measures a home’s energy usage, for example, could reveal how many people live in a home, their daily routines, what types of appliances are used in the home, and even more personal details such as hygiene habits, medical needs, and interactions with others. 51 Similarly, the average car, through a combination of GPS technology and Event Data Recorders (EDR’s), could record the frequency and location of an individual’s driving habits, such as doctors appointments, personal visits, or daily lunch routines. 52 More and more household smart devices—such as TV’s, phones, speakers, and thermostats—are incorporating voice-activation technology, fueling concerns among privacy advocates that people’s private conversations and activities could be monitored. 53 Likewise, a device attached to the skin, such as a galvanic skin response monitor, that measures the physiological signals and emotional arousal of users could conceivably be used by third parties to detect, in real-time, whether that user is nervous, in pain, or even lying. 54 In short, the concept of “quantified self” could expand enormously to create rich behavioral profiles. Moreover, through data enrichment mechanisms, unexpected insights may now be drawn by combining

48. REBACK & COSTELLO, supra note 21, at 2.
50. FTC IoT Report, supra note 9, at 15.
52. Id. at 12.
53. Samantha Murphy Kelly, Samsung’s TVs Aren’t the Only Devices Listening to You, MASHABLE (Feb. 10, 2015), available at http://mashable.com/2015/02/10/smart-devices-listening/#qjTeX1teo5qD. In the case of Samsung, the terms and conditions governing Samsung’s SmartTV voice control stated “that if your spoken words include personal or other sensitive information, that information will be among the data captured and transmitted to a third party through your use of Voice Recognition.” Id. Following public uproar over these terms, Samsung clarified that this would only be transmitted to a third party in order to directly assist with a voice command and not for any other purpose. Id. Samsung also stated that the microphones were only listening for a particular activation phrase or keyword that initiates the Voice Recognition software; once the software was initiated and the voice command task had been completed, it would not collect or transmit any other data. Id. Similar technologies and policies are in place with Nest’s smart thermometers, Apple’s iPhones, and Amazon’s Echo Speaker. Id.
54. ANDERSON & Raine, supra note 20, at 45.
data sets from these myriad IoT devices. Originally insignificant data collected through a single device can later be used with other data to infer information with a totally different meaning.

IoT device data that can be used as a persistent identifier, especially when combined with other personal data, could also make it impossible to remain anonymous. Through IPv6, the most recent version of the protocol that assigns IP addresses, every single IoT device can now have its own IP address—a unique, persistent identifier that can be used to track an individual device across multiple networks. Even further, by analyzing such things as a device’s typical proximity to other devices, the IP addresses of multiple IoT devices can be linked together to create a unique “digital fingerprint” that is attributable to a single individual. This fingerprint would enable IoT stakeholders to track a user across devices and throughout their day-to-day life. Even anonymized data, which is not protected as “personally identifiable information” under most privacy laws, is now increasingly vulnerable to re-identification. Powerful algorithms that combine thousands of different data points across IoT devices have raised concerns that any information that distinguishes one person from another can conceivably be used to re-identify anonymous data.

In essence, the IoT could lead to a perfect storm because of its “ubiquitous networking platforms; the huge proliferation of addressable things made possible by IPv6; and the out-of-sight-out-of-mind nature of many of the ‘things’ in question.” As Google’s CEO recently noted, the IoT will become so omnipresent that people “[will not] even sense it; it will be part of [their] presence all the time.” The potential for unwanted intrusion by third parties is much greater in an environment where people are in constant proximity to self-monitoring devices, which are broadcast to smartphones and linked to social media accounts for geolocation and social interaction, all of which provide the opportunity to monitor individuals’ behavior and movements remotely and in real-time. There is a heightened risk that the data will be accessed and used in

56. EU IoT Report, supra note 47, at 7.
59. EU IoT Report, supra note 47, at 11.
60. Narayanan & Shmatikov, supra note 57, at 26; EU IoT Report, supra note 47, at 8-9.
61. Anderson & Raine, supra note 20, at 44.
63. Anderson & Raine, supra note 20, at 45, 48.
illicit ways. In this vein, according to some commentators, the IoT could set the stage for “extraordinarily targeted monitoring and manipulation of individuals.”

The IoT is thus redrawing the boundaries of what constitutes “personally identifiable information,” and fundamentally challenging the way we address data privacy concerns. Unfortunately, most global privacy laws are ill-equipped to cope with this evolution. The U.S. in particular has no single, comprehensive federal law regulating privacy or processing of personal data generally. Instead, there is a fragmented and evolving patchwork of federal and state laws and regulations, as well as common law principles, that overlap, complement, and sometimes contradict one another. Federal laws and regulations are mostly limited to specific industries or particular types of data. The Gramm-Leach Bliley Act, for example, regulates financial institutions’ management of nonpublic personal information, while the Health Insurance Portability and Accountability Act of 1996 (HIPAA), as updated by the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH), protects the privacy and security of personal health information handled by healthcare providers and certain other covered entities. Businesses whose activities do not fall within the limited scope of these statutes, but nonetheless collect and process consumer personal data, likely fall under the jurisdiction of the FTC, which actively regulates consumer privacy and information security issues under the Federal Trade Commission Act of 1914 (“FTC Act”), a consumer protection law that prohibits unfair or deceptive commercial practices. In particular, the FTC routinely brings enforcement actions against companies for failing to comply with statements made in their posted privacy policies and providing inadequate security measures for safeguarding consumer information. Without any statutory direction, companies are forced to comb through the complaints and consent decrees that the FTC files in relation to these enforcement actions to ascertain the privacy and data security standards. Additionally, the FTC and other government agencies, as well as industry self-regulatory groups, have also developed

64. Id.
68. Other privacy-related statutes that govern certain industries or particular forms of data processing include: the Fair Credit Reporting Act of 1970 (15 U.S.C. §§ 1681–1681x (2012)), which regulates the privacy of consumer report information, including credit information; the Telecommunications Act of 1996 (47 U.S.C. § 222 (2012)), which protects the privacy of customer proprietary network information obtained by telecommunications carriers; the Children’s Online Privacy Protection Act of 1998 (15 U.S.C. §§ 6501–6506 (2012)), which regulates the online collection of information from children; the Video Privacy Protection Act of 1998 (18 U.S.C. § 2710 (2012)), which protects the disclosure of personally identifiable rental records of prerecorded video cassette tapes or similar audio visual material; and the Cable Television Privacy Act of 1984 (47 U.S.C. § 551 (2012)), which regulates the privacy of personally identifiable information obtained from cable television subscribers.
guidelines—not binding law—that are considered best practices and/or industry standards.

What each of these statutes and guidelines have in common is their continued emphasis on the Fair Information Practice Principles (“FIPPs”). Traditionally, data privacy concerns have been addressed through FIPPs, a set of malleable yet widely accepted privacy principles that have developed over time and across jurisdictions. These principles are deeply rooted in U.S. and EU privacy laws as high-level guideposts, and they form the basis of oft-cited international privacy frameworks. While individual notice and consent are the two bedrock principles that consistently shape the collection, use, and disclosure of personal information, other important FIPPs include: (1) Data Minimization (i.e. collection limitation): organizations should limit as much as possible the amount of personal data they collect about individuals; (2) Purpose Specification: organizations should specify the purposes of collecting personal data prior to, or at the point of collection; and (3) Use Limitation: organizations should only use personal data for the purposes originally specified and should destroy or discard such information when it is no longer necessary for such purposes.

The problem with FIPPs is that, while these principles have served as the basis for how we conceptualize privacy in the digital age, they are currently applied in ways ill-suited for the coming IoT. The interaction between objects, between individuals and other objects, and between objects and back-end systems will result in the generation of data flows that can hardly be managed with classical data privacy tools. Today, most consumers only give a passing glance at privacy notices, end-user license agreements, and other terms of use before accepting those terms and moving on. One recent study indicated that few consumers actually read online privacy policies, and doing so would take over 200 hours per year for the average Internet user. Yet, the IoT could significantly amplify consumer protection concerns given the dramatically increased potential for commercial data collection and individual profiling. Even the minimal level of privacy protection afforded by publicly available privacy statements will be swallowed whole by the omnipresence of connected objects engaged in constant data processing and sharing functions. It is unrealistic to expect that individuals will be willing or able to register their

71. Id. at 3.
72. Id.
73. EU IoT Report, supra note 47, at 6.
75. ANDERSON & RAINÉ, supra note 20, at 45.
informed preferences in the potentially hundreds or thousands of times a day they come across a new connected device; that would not only be incredibly burdensome for individuals but would also slow down the data transmissions underlying the IoT.\textsuperscript{76} Furthermore, for the many IoT devices that lack interactive screens or user interfaces, notifying and obtaining adequate consent from users is all but impossible.\textsuperscript{77}

Even assuming the particular device could actually deliver a traditional privacy notice, what individual should consent to those terms? To whom should the privacy policy apply? Many IoT devices will be shared among family and friends, or even resold to different users; in these situations, the person operating the device is not necessarily the original owner or registered user that had the opportunity to weigh the particular privacy considerations and provide consent.\textsuperscript{78} Similarly, the number of stakeholders involved in the IoT ecosystem—including device manufacturers, third-party application developers, data platforms, device lenders, social media platforms, data brokers, third-party service providers, and cloud service providers, among others—will inevitably create confusion among users themselves over which stakeholder’s privacy policy applies to a specific piece of data, or which stakeholder to contact in order to access or correct data, or even which stakeholder to hold responsible in the event something goes wrong. As the Future of Privacy Forum noted, to ask individuals to police their own privacy in an era of constant data communications among numerous stakeholders is “akin to [telling] Sisyphus that he can rest as soon as he gets that rock to settle atop the hill.”\textsuperscript{79}

Consumers are not the only ones that will be disadvantaged by the current application of FIPPs. As a business, the power of the IoT is in the data: by combining and analyzing vast datasets, companies can gain new insights and develop new products and services, and create other revenue-generating opportunities. However, the principles of purpose specification, data minimization, and use limitation require organizations to specify upfront the particular purposes for using the data, collect only the data needed to achieve those purposes, and limit use of the data only to those specified purposes. Companies cannot possibly prophesize the new and valuable ways to use the massive volumes of data they collect years down the line; yet, as it stands now, businesses that originally promise not to use or share data in a certain way will risk an enforcement action if they later choose to do so.\textsuperscript{80} It is equally unrealistic to expect businesses to provide consumers with notice and choice each time they find a new use for data, particularly in an era of ubiquitously connected devices and ever-shifting end-users. If it is not possible to control the interaction of

\textsuperscript{76} WOLF, supra note 70, at 4.
\textsuperscript{77} FTC IoT Report, supra note 9, at 22.
\textsuperscript{78} WOLF, supra note 70, at 4.
\textsuperscript{79} Id.
\textsuperscript{80} OHLHAUSEN, supra note 2.
myriad objects or create virtual boundaries, it will be equally impossible to control data flows and subsequent uses of data.\footnote{EU IoT Report, supra note 47, at 6.} It is thus necessary to begin consideration of a new approach to addressing privacy concerns in the IoT, one that is not beholden to the outdated principles of notice, choice, data minimization, and purpose limitation, but on use and security.

Much like consumers, businesses will also inevitably have difficulty determining who, among the multiple IoT stakeholders involved in data processing activities, is responsible for compliance with data protection rules. The concepts of “data controller” (the person or entity that determines the purposes and means of processing personal data) and “data processor” (the person or entity that processes data on the controller’s behalf) play a crucial role in EU privacy laws because they determine who is responsible for compliance, how data subjects can exercise their rights, and which national law applies.\footnote{Id. at 1.}

But, with so many actors involved, either simultaneously or at different stages of a product’s lifecycle, it is difficult to determine which data processing operations are connected and which operations have different purposes. As a result, businesses will often be unsure who amongst them should be considered a “controller” and who should be considered a “processor.” If it is not sufficiently clear what is required from whom, there is an obvious risk of diffusion of responsibility for data protection compliance.

To prepare for this looming storm, companies are looking to the FTC’s reports and past consent decrees as authoritative guidance on these issues. While the FTC recently acknowledged that traditional privacy principles might need to be adjusted in the IoT era, it also professed its continued belief in the relevance of those principles.\footnote{FTC IoT Report, supra note 9, at 33, 39.} In particular, the FTC continues to emphasize the following three core tenets:

- **Privacy by Design**: Companies should incorporate substantive privacy protections throughout the lifecycle of their products and services, including data security, reasonable collection limits, sound retention and disposal practices, and data accuracy.

- **Simplified Consumer Choice**: While no consumer choice is required for data collection that is consistent with the context of a transaction or an existing customer relationship, companies should otherwise enable consumers to make a simple decision about their data. Affirmative consent should be obtained when: (1) collecting sensitive data for certain purposes and (2) using consumer data in a significantly different way than originally claimed.

- **Transparency**: Companies should increase the transparency of their data practices by providing consumers with shorter and more

The devil, of course, is in the details: it remains to be seen whether or not these principles will hold up in the IoT era. For example, the FTC may disagree with businesses over what is, and what is not, “consistent” with the context of a transaction or existing business relationship. Without more detailed guidance, companies will need to walk a thin line to avoid an enforcement action or consumer backlash.

In its 2014 report on Big Data, the White House suggested that, as the trajectory of technology shifts toward far more collection and use of data by entities that lack a direct relationship with an individual, the focus should shift away from the “notice and consent framework” and towards a “responsible use framework.”\footnote{EXEC. OFFICE OF THE PRESIDENT, BIG DATA: SEIZING OPPORTUNITIES, PRESERVING VALUES 55–56 (2014), available at https://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf.} This framework would emphasize the context of data use, holding “data collectors and users accountable for how they manage the data and any harms [they cause], rather than narrowly defining their responsibility to whether they properly obtained consent at the time of collection.”\footnote{Id. at 56 (emphasis added).} Such an approach would also shift responsibility for managing privacy away from the individual, who is not well-equipped to understand or dispute many consent notices, and toward the entities that are collecting and using the data.\footnote{See, e.g., WOLF, supra note 70, at 7–12 (advocating a “use-based privacy paradigm”).} Other organizations have also endorsed such an approach as a way to better balance the socially beneficial uses of the IoT and Big Data with the increased privacy risks to individuals.\footnote{See OHLHAUSEN, supra note 2.}

In recent remarks, FTC Commissioner Maureen Ohlhausen may have signaled the future of FTC enforcement, noting that it could be useful to look at the potential harm that may result from different types of data use rather than imposing strict prohibitions.\footnote{See OHLHAUSEN, supra note 2.}

In the meantime, however, IoT businesses should seek creative solutions for providing consumers with the requisite notice and choice. While the FTC acknowledges the practical difficulty of complying with these requirements for IoT devices, it has offered some solutions, including video tutorials for privacy settings; affixing a QR code or similar barcode that, when scanned, will take consumers to a website that provides information about privacy practices and enables choices; a set-up wizard that describes privacy practices and allows users to configure devices; and “out-of-band” communications requested by...
consumers, such as emails or texts. Likewise, the U.K.’s Information Commissioner’s Office has indicated that companies can overcome the challenges of providing notice to individuals by using lights, buzzers, or other signals to indicate ongoing data processing. These tools can also be useful to other individuals in the vicinity of the IoT device that may be subject to personal data collection.  

Companies should also monitor the innovative solutions being offered in the marketplace to manage user privacy in the IoT era. The User-Managed Access protocol (“UMA”), for example, allows individuals to customize privacy settings for their own data across multiple applications through the use of a centralized service. Individuals can affirmatively choose to share selected portions of their data directly with any parties that utilize the UMA protocol. They can also revoke a party’s authorization to access their data whenever they see fit. Moreover, by visiting a single online control console, individuals can set, view, or alter their sharing preferences at will. Because the protocol is standardized, it is designed so that companies can work with the same protocol and achieve interoperability. Such a system not only provides consumers with real choice through a convenient central dashboard, it also protects businesses by going beyond the minimum that is required by current privacy regulations.

In a similar vein, another company has worked with the Online Trust Alliance to develop a tool that helps IoT manufacturers create a customized, consumer-friendly privacy policy and display it on an easy-to-read dashboard. Beyond legitimate notice and consent, businesses implementing IoT projects should ensure that roles and responsibilities among various stakeholders are clearly allocated. Contractual arrangements should address situations where there is joint control of data, specifying who is legally responsible for data

92. Id. The author provides the following example:

Imagine a health data-sharing ecosystem in which service providers such as Dr. Bob’s BHealthy practice and devices such as the Beat blood pressure monitor work with Alice’s UMA service, called ShareHub. She can hit the UMA-enabled Share button in the BHealthy portal to share the allergy portion of her health record with her husband Ted ahead of an overseas trip she’s taking and manage that preference through ShareHub. Separately, Alice can hit Share in the portal of the Beat blood pressure monitor service to ensure Dr. Bob gets an ongoing view of her blood pressure and then manage that preference through ShareHub. Alice can visit ShareHub any time she wants to update her privacy settings. She can remove her previous doctor’s authorization and ensure her new doctor gets access. Id.

93. Id.
protection rules and responsibilities, and who will bear the financial consequences of any damage to the consumer. Companies should be careful to select only those partners and suppliers that offer, at a minimum, reasonable and industry-standard warranties and other contractual commitments with respect to privacy and data protection.

V. SECURITY

As the number of Internet-connected objects expands, so too does the potential attack surface. The IoT faces serious security issues because it is based on interoperability and interdependence: more interactions among devices lead to more areas of vulnerability.95 Sophisticated attacks can “spread widely in very little time, precisely because IoT systems are doing exactly what they are built to do—spread out widely and interoperable across different programs and devices.”96 The IoT will thus create new areas susceptible to cyber attacks designed to either compromise the device itself or gain access to the network it shares with other devices. To make matters worse, many IoT objects, such as household appliances, are still not programmed with an eye toward security, and many of the manufacturers of these objects may lack the experience or expertise to implement safeguards.97 Similarly, because of their small size, many IoT objects lack the resources available to implement appropriate security measures.98 A study recently released by Hewlett-Packard in 2014 found that at least 70 percent of IoT objects are seriously vulnerable to attacks.99

The security challenges stemming from the IoT ecosystem are innumerable. Consider, for example, the issue of incorporating IoT applications into a company’s older (legacy) computer equipment. Replacing or upgrading legacy systems is often a suboptimal option for businesses because the process can be cost-prohibitive and significantly disruptive to business operations and mission-critical security.100 Instead, companies frequently choose to integrate IoT solutions into their current enterprise resource management system by layering them on top of existing legacy systems. Yet, many of these legacy systems—

95. KOMINERS, supra note 31, at 17.
96. Id.
97. REBACK & COSTELLO, supra note 21, at 3.
98. CTIA Report, supra note 30, at 11.
100. A recent Ponemon Institute study found that, in a survey of 599 IT security executives in 13 countries from the utility, oil and gas, alternative energy, and manufacturing sectors, 54% of companies were not confident or unsure if they could “upgrade legacy systems to the next improved security state in cost-effective ways without sacrificing mission-critical security.” See Kate Vinton, Hacking Gets Physical: Utilities at Risk for Cyber Attacks, FORBES (July 10, 2014, 3:22 PM), http://www.forbes.com/sites/katevinton/2014/07/10/hacking-gets-physical-utilities-at-risk-for-cyber-attacks/#2715e4857a0b4f5372ac6b30.
such as the industrial controls involved in supply-chain management—have been in operation for decades and may not have been initially designed for web connectivity. As a result, these systems typically run on out-of-date software with security vulnerabilities that are often difficult to patch or upgrade. With the myriad points of communications introduced by IoT applications and devices, the inadequate security controls associated with these older programs make them attractive entry points for disruptive attacks.

More fundamentally, the IoT ecosystem is diverse and distributed broadly across multiple industries. Likewise, the range of IoT objects or devices is equally diffuse, including anything from glucose meters and pacemakers, to thermostats and coffeemakers, to RFID tags used for inventory management. These devices depend on a variety of different wireless technologies to communicate with people and each other. With multiple IoT stakeholders operating in differing roles across distinct industries and domains, and with a wide range of devices that rely on different types of computer hardware and communications protocols, appropriate cybersecurity coordination across the IoT ecosystem may be difficult if not impossible, particularly when a set of best practices or guidelines may not translate from one vendor or device to another. Yet, without adequate coordination, an exploitable weakness in one single type of IoT device could suddenly become a problem for many others.

As devices connected through the IoT proliferate, machine-to-machine trust issues will become more serious. A recent study by the Georgia Institute of Technology noted that, while humans learn how to determine if another person is trustworthy through information gained by perception, memory and context, it is unclear whether those concepts can be transferred to the digital realm. Smartphones—now the mobile hub of peoples’ lives—need to determine on behalf of their users how trustworthy, for example, a smart-watch or intelligent security camera may be; self-driving cars will need to communicate with each other and distinguish between spoofed communications, illogical commands, or even software in other cars that has not been updated with the latest security patches. All of this must be accomplished automatically without human intervention; yet, given the heterogeneous, uncoordinated manner in which the IoT ecosystem is developing, accomplishing effective trust between and among disparate devices and objects will be difficult.

The IoT’s evolution has also raised the stakes of a successful security breach. Everyday objects like televisions, thermostats, and coffeemakers can now be

---

103. *INST. FOR INFO. SEC. & PRIVACY*, supra note 74, at 10.
104. *Id.* at 12.
105. *Id.* at 10.
106. *Id.* at 10.
exploited to compromise the personal information that they store and transmit. But even beyond that, there is a risk to physical safety: IoT devices and data can now literally provide a window into an otherwise private space. For example the FTC recently settled charges with TrendNet, a marketer of Internet-connected home security video cameras, alleging that its lax security practices exposed the private lives of hundreds of consumers to public viewing on the Internet. The video feeds apparently displayed babies asleep in their cribs, young children playing, and adults going about their daily lives.\textsuperscript{107} No more than a year after the settlement was reached, a website published more than 73,000 different video feeds from a range of different webcam manufacturers, exposing feeds from users around the world who did not change default passwords.\textsuperscript{108}

Beyond these intrusions into otherwise private spaces, a breach of an IoT object can also result in significant bodily harm. One researcher in an FTC workshop on the IoT noted that he was able to hack two insulin pumps from a remote location and change the settings to deny delivery of medicine.\textsuperscript{109} Similarly, in 2015, two White Hat hackers successfully hacked into and remotely controlled a Jeep Cherokee while it was travelling on a highway miles away.\textsuperscript{110} That same year, the FBI investigated a security researcher for hacking the in-flight networks of commercial airplanes over a dozen times.\textsuperscript{111}

Because IoT devices are designed to interact with the physical world, the impact of an attack could be more severe because of the potential physical devastation.\textsuperscript{112} The IoT has already expanded to industrial society, with the convergence of IT and automation networks in areas like inventory tracking and manufacturing lines. As the National Institute of Standards and Technology (“NIST”) notes, in addition to threatening intellectual property—which is a problem that is common to all IT system vulnerabilities—attacks on a physical system can adversely affect product quality, product performance, and operational safety.\textsuperscript{113} A denial of service attack against a website, for example, could lead to lost data, lost revenue, and even damage to a server; by contrast, “a


\textsuperscript{109} FTC IoT Report, supra note 9, at 12.

\textsuperscript{110} See Andy Greenberg, Hackers Remotely Kill a Jeep on the Highway—With Me In It, WIRED (July 21, 2015, 6:00 AM), http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/.

\textsuperscript{111} Kim Zetter, Feds Say that Banned Researcher Commandeered a Plane, WIRED (May 15, 2015, 10:14 PM), http://www.wired.com/2015/05/feds-say-banned-researcher-commandeered-plane/.


\textsuperscript{113} Id.
denial of service attack against the system that regulates the safe operation of a power generation facility or an industrial plant can lead to irreparable damage to capital equipment that could take months or years to replace.”

As the IoT expands to critical infrastructure systems like transportation systems, water dams, or energy grids of major cities, a security breach could wreak widespread chaos and havoc on businesses and populations. Recently, the security firm Kapersky Labs indicated that targeted attacks on computer industrial control systems are the biggest threat to the U.S.’s critical national infrastructure. Because these systems control physical processes related to vital resources like water, transportation, and power, the effects of any service interruption could be catastrophic. For example, the Stuxnet attack—widely considered to be one of the first cyber attacks on critical infrastructure systems—utilized a computer worm that infected the software of at least 14 industrial sites in Iran, including a uranium enrichment plant. In particular, the worm targeted the software used to program a specific type of industrial control system operating Iranian centrifuges. The worm ultimately took control of the centrifuges, causing them to spin wildly and tear themselves apart, all while sending phony monitoring signals to the human operators of the plant to indicate that processes were functioning normally. This groundbreaking cyber attack caused millions of dollars in damages to Iranian centrifuges and delayed their enrichment program for years. Stuxnet is a sober reminder not only of the dangers to industrial control systems’ software and devices but also of the unique large-scale risks inherent to the IoT as it continues to bridge the physical world with the virtual world. According to NIST, “malware with capabilities similar to those displayed by Stuxnet could maliciously alter the operational state of any cyber physical systems by compromising cyber subsystems . . . in ways that adversely affect safety, reliability, resilience, privacy and financial bottom lines.”

Despite these risks, the U.S.’s regulatory approach to IoT cybersecurity in the near future is likely to be piecemeal and reactive. The automated car industry, for example, witnessed a flurry of potential regulatory activity after reports were published that White Hat hackers had hacked a Jeep Cherokee and

---

114. Id.
117. Greenberg, supra note 110, at 60.
120. Greenberg, supra note 110, at 67.
remotely tampered with its brakes, steering and engine while traveling on a highway. Two senators recently introduced the Your Car (SPY) Act, that would direct the National Highway Traffic Safety Administration and the FTC to create federal standards to secure connected cars and protect drivers’ privacy. Likewise, in December 2015, the California Department of Motor Vehicles announced a list of draft regulations for autonomous vehicles, many of which pertain to the security of the car as well as the types of non-safety-related data collected from those cars. The regulations would require the vehicles to be able to detect, respond, and alert the operator to cyber attacks, while also providing the operator with the capability to override the autonomous technology in the event of an alert. Similarly, amidst concerns over airplane safety, the Government Accountability Office (GAO) released a report outlining potentially critical vulnerabilities to newer planes. According to the report, because these planes have a single network that is used both by pilots to fly the plane and passengers for their Wi-Fi connections, a hacker could conceivably use the Wi-Fi connection to hack into the avionics and remotely control the plane.

In response to these perceived vulnerabilities, the GAO’s report called on the Federal Aviation Administration (FAA) to address possible cybersecurity concerns through aircraft certification standards.

Given that the cyber threat landscape continues to evolve and adapt in a dynamic and often unpredictable fashion, it is doubtful that regulators will commit to comprehensive cybersecurity legislation with prescriptive rules in the near-term. Rather, lawmakers and regulators will likely push for industry-
specific regulations with broad, even vague security standards, leaving it up to the private sector or the industry to determine what practices best meet those standards. In this environment of regulatory uncertainty, businesses—particularly those not governed by industry-specific laws or regulations—should closely monitor non-binding cybersecurity frameworks and self-regulatory initiatives developed by influential, multi-stakeholder efforts. For example, in September 2015, NIST published a draft of its comprehensive IoT framework, entitled the “Framework for Cyber-Physical Systems” (the “CPS Framework”). The CPS Framework seeks to create a shared understanding of Cyber-Physical Systems (“CPS”)—defined broadly as interacting networks of physical and computational components—by providing a high-level examination of the various issues facing CPS, including privacy and security. Based on input from many experts, the CPS Framework also offers a standardized, cross-industry blueprint with common language and recommendations that companies can utilize to confront these issues. Similarly, the nonprofit Online Trust Alliance commissioned a multi-stakeholder initiative, including several major companies, to develop an “IoT Trust Framework” that provides prescriptive advice to manufacturers and developers on privacy and security best practices throughout the lifecycle of IoT products, including those products that might be used by multiple users or transferred to new owners. The OTA Framework, currently in draft form, now has over 30 measurable and enforceable criteria regarding: (1) security, (2) user access and credentials, and (3) privacy, disclosures, and transparency. The OTA’s goal is to develop an international IoT certification program that uses this self-regulatory code of conduct to certify IoT companies as trustworthy in the areas of privacy and security. Each of these frameworks could be used as a comprehensive roadmap for IoT companies to incorporate privacy and security best practices that comply with regulatory expectations.

In addition to these non-binding guidelines, the FTC has issued numerous guidelines on implementing “reasonable” technical, physical, and administrative security measures. In particular, the FTC strongly encourages IoT companies to

growth of IoT in the U.S., which would “recognize the importance of consensus-based best practices” and the “important role” that “businesses can play…in the future development of the [IoT].” See S. Res. 110, supra note 26. The House of Representatives passed a similar resolution in April 2015, recommending that Congress “only address discrete harms in the Internet of Things marketplace when identified pursuant to a cost-benefit analysis revealing that governmental action is necessary.” See H.Res. 195, supra note 27.

127. Greenberg, supra note 110.
128. Id.
130. OTA Releases, supra note 129.
adopt a “security by design” approach by building security into the IoT product at the outset and at every stage of its development.\textsuperscript{131} This includes, among other things, conducting periodic privacy and security risk assessments that consider the risks of collecting and retaining personal information; incorporating the use of smart defaults—for example, requiring consumers to change default passwords—during the set-up process of IoT devices; and periodically reviewing and testing security measures, including prior to launching a product.\textsuperscript{132} The FTC’s recently released guidance also sheds light on how it expects businesses to build security into IoT products through a risk-based approach. The publication explains best practices developed by security experts, such as the use of strong encryption for data in transit and in storage, proper authentication techniques, and permission-based controls that limit access to data, among many other tools.\textsuperscript{133} The FTC also emphasized that it is crucial for companies to implement: (1) a defense-in-depth approach that incorporates security measures at several levels; (2) accountability mechanisms for data security that begin at the executive level; and (3) rigorous monitoring and testing of connected devices throughout their expected lifecycle.\textsuperscript{134}

It is this last recommendation, however, that is perhaps the most difficult for IoT companies to successfully implement. Even if companies regularly monitor and test their devices for security vulnerabilities, how can they establish an effective approach for updating and patching their security? Security flaws in the software of IoT objects are already being discovered and exploited faster than they can be managed and patched.\textsuperscript{135} The FTC likes to emphasize that security is not a “one-and-done” proposition. Yet, as security vulnerabilities are found in the countless number of IoT devices “in the wild,” how can companies keep track of these devices and ensure that security updates or patches will be delivered to end-users that could number in the millions?\textsuperscript{136} Even if companies can update their network-level security measures to better protect against known threats, end-users themselves usually have to manually download and install relevant software patches.\textsuperscript{137} As a result, there is not an effective channel to reach the majority of devices in a timely fashion.\textsuperscript{138} To make matters worse, certain IoT

\begin{footnotesize}
\begin{enumerate}
\item[131.] FTC IoT Report, supra note 9, at 28.
\item[132.] Id.
\item[134.] Id.; see also, FTC IoT Report, supra note 9, at 28–31.
\item[135.] Kam, supra note 101.
\item[137.] Id.
\item[138.] See Michael Coates, The Internet of Things Will Be Vulnerable for Years, and No One is Incentivized to Fix it, VENTUREBEAT (April 23, 2014, 8:30 AM), http://venturebeat.com/2014/08/23/the-internet-of-things-will-be-vulnerable-for-years-and-no-one-is-incentivized-to-fix-it/.
\end{enumerate}
\end{footnotesize}
manufacturers often lack an economic incentive to provide software updates and support: manufacturers of specialized computer chips, which are cheap and operate on a thin profit margin, are typically working on or shipping the next version of the chip, while the original device manufacturers—who often do not get their brand name on the finished product—are working to upgrade their product to support the new chip.\textsuperscript{139} In this mindset, where getting the product to the market is the overwhelming priority, security may not be a priority.

All of this makes “security by design” a critical strategy for developing and marketing an IoT product. The entire product must be designed and maintained with an eye toward security. This means partnering with reputable device and chip manufacturers that consider security from the outset and offer appropriate warranties for their products. Even if manufacturers do adopt this approach, it will still be an uphill battle: as one IoT expert recently asserted:

\begin{quote}
[h]ackers can easily purchase any IoT device, which will often contain the same security features of other, identical devices already deployed in hundreds or even thousands of homes. Unlike servers or networking equipment, which are usually hacked through remote access points and reside in protected and monitored environments, IoT devices are more accessible to malicious threat actors.”\textsuperscript{140}
\end{quote}

Regardless, while no IoT product will be infallible, a commitment to “security by design” may at least help guard against civil liability and regulatory enforcement by signaling a reasonable effort on the part of the company to secure the product and the corresponding data it collects.

In addition, when feasible, software updates or patches should be made available to end-users as seamlessly as possible.\textsuperscript{141} Even if a company issues a new version of an IoT product, it should still carefully consider its obligations to customers that bought earlier versions of the product, including how long it should offer security updates or technical support.\textsuperscript{142} End-users should also be notified about important security information in real time, whether that be through electronic messages to registered users, a published notice on a company website, or “on-the-product” alerts.\textsuperscript{143}

Beyond considering the security of their own product, IoT businesses should work to ensure that all third-party service providers that handle its sensitive data


\textsuperscript{142} \textit{Id}.

\textsuperscript{143} \textit{Id}. 

are capable of maintaining reasonable security measures. In the U.S., organizations are generally legally responsible for the actions of third parties that process data on their behalf (i.e., “data processors”). A company’s privacy and cybersecurity obligations, as well as any public statements it makes about its privacy and cybersecurity practices, apply equally to any third parties that have access to a company’s data and IT assets. It is thus crucial for businesses to maintain proper oversight of a service provider’s compliance with privacy and cybersecurity obligations, including site inspections, audits, and assessments. A failure to do so could result in an FTC enforcement action. Contracts with service providers should mandate such oversight. In addition, agreements with service providers should prohibit the providers from using customer data for their own purposes, limit the conditions under which they can share such information, and require them to implement appropriate security measures. Proper “Terms of Service” and “End-User” agreements can also help protect IoT companies from liability by defining the role of the end-user of an IoT device in helping to maintain a secure environment and comply with applicable legal obligations.

As with the current privacy paradigm, it remains to be seen whether these principles will be sufficient to keep IoT products—and end-users—safe from attack. According to a study by the International Data Corporation (IDC), 90% of all IT networks will have an IoT-based security breach within two years. Critics are increasingly skeptical: with more devices, more sophisticated attacks, viruses spreading faster on the Internet, less technical expertise, and vulnerabilities that are difficult if not impossible to patch, many believe we have an “incipient disaster” looming. According to the top analyst at NIST, the interconnectivity and complexity of the IoT “leaves public and private computer systems essentially indefensible, and no amount of security guidance can provide salvation.”

Amidst such drastic assessments, companies seeking to get involved in the IoT revolution must be prepared to vigilantly monitor the security of their devices and data, and address new security issues that arise in real time. A enterprise-wide incident response plan—a set of policies and procedures that specify how an organization will address and manage a security incident in order to mitigate the damage—will increasingly become an essential operational component for the growing number of organizations that are integrating IoT

144. Id. at 7.
146. See id.
148. Schneier, supra note 139.
technology into their business. The potential costs of a breach are already substantial and wide-ranging. A company that suffers a significant breach could face, among other things: exposure to class action liability; regulatory enforcement and fines; reputational damage; loss of customers; loss of revenue, intellectual property theft; and additional expenses related to responding to a breach, like hiring forensic investigators, offering credit monitoring to victims, and remediating security vulnerabilities. But as the overwhelming number of IoT devices—many of which hold sensitive data or control industrial operations—continues to grow at a rate that eclipses security capabilities, these costs will become more frequent and more pronounced for businesses. In fact, the costs associated with U.S. regulatory compliance alone could be astronomical for IoT entities. With the exception of three states,150 each state and the District of Columbia151 has its own data breach notification law that requires data owners and data licensees to provide notice to affected consumers, and possibly government agencies, following a security breach of certain personal data.152 The statutory requirements for these laws differ with respect to many elements, including: the definition of “personal information” and “security breach”; the level of harm that requires notification to individuals; whom, when, and how to notify in the event of a breach; and exceptions to the notification obligation.153 Several states also have their own information security regulations that impose minimum information security requirements on businesses that either operate in that state or possess personal information of residents of that state.154

150. Alabama, New Mexico and South Dakota currently do not have data breach notification laws.


152. See sources cited supra note 151.

153. Id.

154. Id.
Massachusetts, for example, requires businesses holding certain personal information about its residents to adopt several prescribed administrative, physical, and technical security controls. As with the state data breach notification laws, these regulations will differ in many ways, including to whom the regulation applies, the types of information that must be protected, and the types of safeguards that must be implemented. IoT entities will thus need to implement, coordinate, and prepare for a vast maze of differing regulatory requirements, particularly with respect to consumer-driven IoT devices that could conceivably collect data about an individual in any state. While the administrative burden of managing these obligations could be daunting, it still pales in comparison to the potential costs of litigation and regulatory enforcement that could result from non-compliance.

Even if security breaches are inevitable, companies that thoroughly prepare from the outset and follow the guidance of applicable regulators are significantly more insulated from these risks than the ones that do not.

VI. OTHER ISSUES

A. Default Warranties

Under the Uniform Commercial Code (“UCC”), which governs contract law, not tort law like products liability, software is generally viewed as a “good,” which means that the normal warranties of goods apply. This not only includes any express warranties the seller makes about its products—at the point of sale, in product literature, or anywhere else—it also includes implied warranties of “merchantability” and “fitness for a particular purpose” that are incorporated into every good by default. Under the latter warranty, if a buyer relies on the seller’s skill or judgment in selecting a suitable good, there is an implied warranty that the item will, in fact, be suitable for the purpose intended. Because almost all software transactions involve reliance by an unknowledgeable end-user on the seller’s skill and judgment as to what the user needs, this warranty will almost always apply. As a result, any seller of an IoT product must be mindful of the default warranties that apply to its embedded software. These warranties are buyer friendly, and a court may award incidental and consequential damages in the event of their breach. It is important that an IoT seller disclaim all such implied warranties in conspicuous and specific language in any agreements with the end-user. However, even if the seller disclaims implied warranties in writing, companies should keep in mind that many states have consumer protection

157. Id.
158. Id.
stated that prevent waiver of such warranties.\footnote{Id. \S 27:11.} Some states also forbid companies from disclaiming or limiting a buyer’s right to recover incidental or consequential damages from the seller.\footnote{Id.}

**B. Products Liability**

As the Internet infiltrates areas of the physical world not previously affected, it could reshape the law of products liability by redefining who can be held at fault and who will bear the financial consequences if something were to go wrong with a product.\footnote{O’Brien, supra note 16.} Products liability refers to the liability of different parties along a product’s chain of distribution for any damage caused by that product’s defects.\footnote{Id.} A party can be held liable for a product under a number of different legal theories, including “strict products liability,” negligence, and breach of warranty.\footnote{Id.} Often, products liability is a “strict liability” offense, meaning that liability does not depend on the degree of care exercised by the defendant; rather, the defendant is automatically liable once it is proven that the product was defective, even if all possible care was exercised in the preparation or sale of the product.\footnote{Id.} Traditionally, fault flows up the chain of distribution from the retailer to the suppliers and ultimately to the manufacturer.\footnote{Id.}

In contrast to the UCC and contract law, however, software is generally not considered a “product” under the tort law of products liability.\footnote{Seldon J. Childers, Don’t Stop the Music: No Strict Products Liability for Embedded Software, 19 U. Fla. J.L. \\& Pub. Pol’y 125, 161 (2008).} As it stands now, courts typically refuse to apply strict products liability to software defects, reasoning that software is a “service,” not a “product.”\footnote{Id. at 156–57.} To date, software vendors have thus largely avoided strict liability for defects.\footnote{Id.}

But what about an IoT device, where software is embedded in a product rather than sold or licensed on its own? What happens if something goes wrong with an IoT device? What if the software itself in the device is defective or vulnerable to an attack? Could the software vendor be held responsible? Would the other parties along the chain of distribution be held at fault for a software defect or escape strict liability because software is not a “product?”

Because the IoT, by definition, integrates the Internet with the physical world, if something goes wrong with the software of that object—a breach, a glitch, an outage—it could result in physical damage to property or even personal

\footnotesize\textsuperscript{159} Id. \S 27:11.  
\footnotesize\textsuperscript{160} Id.  
\footnotesize\textsuperscript{161} O’Brien, supra note 16.  
\footnotesize\textsuperscript{162} Id.  
\footnotesize\textsuperscript{163} Id.  
\footnotesize\textsuperscript{164} Id.  
\footnotesize\textsuperscript{165} Id.  
\footnotesize\textsuperscript{167} Id. at 156–57.
injury. The more we rely on smart devices for our own decision-making, the greater the likelihood that a software defect could lead to massive damages or bodily harm. As a result, many have argued that software should be considered a product under products liability law, particularly in the IoT era where software is increasingly an intrinsic component of products that can cause serious physical harm.

But even if software is eventually considered a product that is subject to some sort of tort liability, key questions remain unanswered. For instance, should software be treated as an altogether separate and distinct product from the IoT device it manages or enables? Or should software be considered just another component part of the overall IoT device? As the Internet permeates the physical world, it is becoming more and more difficult to differentiate products from the software that is embedded in them. Yet, this distinction is crucial: if the software is considered a component part, then a traditional products liability analysis would ensue. Under this legal framework, the suppliers or manufacturers of a product’s component parts are held strictly liable for defects in the final product along with the finished good manufacturer, even though the finished good manufacturer makes all the design and manufacturing decisions, and the component suppliers may have no idea how its components were used. By extension, if software were considered a component product of the IoT object it is embedded in, this would open the door to hold software component providers strictly liable in the same way that manufacturers of other kinds of products are held strictly liable for defects, regardless of negligence. For example, if the software powering the braking system of a car is defective, and the law defines the embedded software as a component part of the automobile, then both the automobile manufacturer and the component software suppliers and manufacturers may be strictly liable for injuries caused when the software malfunctions and the device causes harm.

A recent products liability suit against a car manufacturer highlights this difficulty of distinguishing between a product and the software embedded within the product. Shortly after the hacking of the Jeep Grand Cherokee by the White Hat hackers mentioned above, a class action suit was filed against Fiat Chrysler Automotives, the manufacturer of the vehicle, as well as Harmon International Industries, the manufacturer of the vehicle’s “infotainment system,” which provides entertainment and navigation services. The plaintiffs alleged a design

168. Id. at 177.
169. Id. at 152.
170. Id. at 140–41.
171. Id. at 183.
173. Id. at 139–140.
174. Id. at 155.
defect in the vehicle’s computer systems; in particular, plaintiffs claimed that the vehicle’s “infotainment system” was connected to the vehicle’s internal communication network, which controlled the engine and other critical systems. Because the infotainment system was always connected to the internet via 3G cellular service, the White Hat hackers were able to remotely take control of the vehicle’s physical systems. According to plaintiffs, the manufacturers’ failure to isolate the two computer systems constituted a design defect, and not a software failure. Whether the court finds this reasoning persuasive still remains to be seen, but as the line between hardware and software defects become blurred, the categorical protection software currently enjoys from products liability suits could be challenged.

In general, the extension of strict products liability to software is a potentially scary situation for all companies involved in the IoT. Unlike defects of purely physical products, it is arguably “impossible or commercially unreasonable to guarantee that software of any complexity contains no errors that might cause unexpected behavior or intermittent malfunctions, so-called ‘bugs,’” If defect-free software is not possible—and minor errors are thus fully within common expectations—how can we hold all parties along the chain of distribution of Internet-connected objects responsible for such defects, regardless of whether or not they were truly at fault? If software is “unavoidably unsafe,” should IoT providers instead be held to a negligence standard, rather than a strict liability standard that imposes liability without any proof of carelessness? Would it be sufficient for an IoT company to provide a warning to the consumer that software flaws and vulnerabilities may exist? What if the consumer or end-user is partially at fault for failing to install a security patch or using passwords that are easily susceptible to attack? Will the end-user be held responsible at all in the allocation of fault? What issues of privacy will arise in products liability litigation when demands are made by potentially liable manufacturers or suppliers to examine the sensitive data stored in the end-user’s IoT device? The law of products liability will need to evolve to provide answers to these questions.

176. Id. at 5.
177. Id. at 4.
178. Id. at 5.
179. Id. at 5-6; see also Cahen v. Toyota Motor Corp., No. 15 cv-01104-WHO, 2015 WL 7566806, at *1, *10–15 (N.D. Cal. Nov. 25, 2015) (dismissing claims alleging that various automakers equipped their vehicles with computer technology that is susceptible to being hacked by third parties for lack of Art. III standing).
180. UNIF. COMPUTER INFO. TRANSACTIONS ACT § 403 cmt. 3(a) (2002). (explaining that the UCITA defines software as “information” rather than a UCC good, however, the UCITA has not been widely adopted by states).
182. O’Brien, supra note 16.
183. Childers, supra note 166, at 154.
Extending strict products liability to software defects could also dramatically obstruct technological progress for the IoT.\textsuperscript{184} Software developers rely heavily on millions of software components that are widely available over the Internet, either for a licensing fee or for free.\textsuperscript{185} The component software provider usually has no specific idea how that component is ultimately used.\textsuperscript{186} Any extension of strict products liability to software component suppliers could subsequently cause those suppliers to restrict components that were previously easily and freely available.\textsuperscript{187}

Amidst this uncertainty, it is crucial for IoT providers to explicitly determine which parties along the chain of distribution are responsible for the risks of product integration and who will bear the financial consequences for any liability arising from defects. These risks are often addressed between parts suppliers and manufacturers under the terms of supply agreements where the parties make clear any contractual duty to defend and indemnify against damages caused by a defective device.\textsuperscript{188} Assuming a seller of an IoT device could eventually be held liable for software defects, companies should also reevaluate their products liability insurance coverage, which is typically found in general liability policies. These policies often contain broad exclusions that insurers use to deny coverage for any injuries arising out of software coding errors.\textsuperscript{189}

\textbf{C. Terms of Service}

To reduce the risk of liability for product defects, breaches of warranties, or any privacy or cybersecurity claims, IoT companies will need to carefully craft “terms of use” or “terms of service” (ToS) to enforce against the end-users of their products.\textsuperscript{190} But companies seeking to enforce ToS will face the same fundamental problems underlying proper notice and consent for their privacy practices. As the number of Internet-connected objects proliferates, how will companies ensure that end-users will take the time to fully understand and assent to ToS rather than giving them a passing glance and moving on? Furthermore, because IoT products like smart cars, coffeemakers, or thermostats will often be shared or reused during their lifecycle, how will businesses obtain an enforceable agreement from end-users other than the original product purchaser? If a product lacks a user interface, will it even be possible to obtain an enforceable agreement for a ToS?

\textsuperscript{184} Id.
\textsuperscript{185} Id.
\textsuperscript{186} Id.
\textsuperscript{187} Id.
\textsuperscript{188} O’Brien, supra note 16.
\textsuperscript{190} See id.
Because IoT objects are constantly interacting with different users and processing data about them, a traditional “shrink-wrap” agreement enclosed in the physical package of the product may be attacked as insufficient to create an enforceable agreement. Instead, companies will need to find creative ways to utilize electronic ToS’s—through a website, mobile app, or product interface—that legally bind the multiple users of an IoT product. Even “browse-wrap” agreements, which companies frequently rely on for electronic ToS’s, could be attacked as inadequate. Under a browse-wrap agreement, a hyperlink to the full terms of the agreement is typically placed on the main page of the website. The agreement does not require any affirmative assent by the end-user; rather, the agreement typically states that a user’s use of the website itself constitutes consent to the terms. Courts will only enforce these agreements when there is evidence that end-users were put on notice of their terms, which is all but impossible to assume if multiple individuals are using the product.

IoT companies, instead, need to find ways to “bake” or incorporate “the equivalent of a click-wrap” agreement into the functionality of their device. Click-wrap agreements require users to provide express assent to the electronic ToS by clicking an “I agree” box or performing some other kind of affirmative action that meets the requirements of the Electronic Signatures in Global and National Commerce Act (E-SIGN). Click-wrap agreements are almost always enforced by courts as long as they necessitate an active role by the user, and will become increasingly necessary in the IoT era. While these types of agreements will better protect companies from liability, it will still be challenging to obtain assent for products that lack screens or are used by multiple individuals. IT teams and legal counsel should work closely together to ensure that, where possible, the product is designed so that each user must affirmatively assent to the ToS before operating the device, such as through user accounts and login credentials. If the product lacks a user interface where the end-user can check a box or otherwise agree to terms, the product should require the user’s agreement through a website or mobile application prior to enabling functionality.

---

192. Id.
193. Id.
194. Id.
195. Id. at 1176; see also Berkson v. Gogo LLC, 97 F. Supp. 3d 359, 401 (E.D. N.Y. 2015) (“‘[T]erms of use’ will not be enforced where there is no evidence that the website user had notice of the agreement; ‘the validity of the [internet] agreement turns on whether the website puts a reasonably prudent user on inquiry notice of the terms of the contract’” (quoting Nguyen v. Barnes & Noble Inc., 763 F.3d 1171, 1177 (9th Cir. 2014))).
197. See, e.g., Berkson, 97 F. Supp. 3d at 397 (“Clickwrap agreements necessitate an active role by the user of a website. Courts, in general, find them enforceable.”).
198. See Class Action Complaint Demand for Jury Trial at 13–15, Mclellan et al. v. Fitbit, Inc., No. 16-cv-36, 2016 WL 64721 (N.D. Ca., Jan. 5, 2016). Companies should also include a copy of the ToS in the package of the product at the point of sale. Additionally, it is advisable to include a
Companies that obtain enforceable assent to their ToS from each user will be significantly more protected from liability and potential class action lawsuits.

D. Software Monetization

As more and more everyday objects connect to the Internet, the IoT will turn many original equipment manufacturers of hardware and appliances into software providers. Many companies that are relatively unfamiliar with the business opportunities of software-embedded devices will not be prepared to protect and monetize their intellectual property rights in that software. Through commercial software licenses, IoT companies in any market can control access to the functions and features of their products and otherwise grow new revenue streams. In particular, through software licenses, companies can, among other things, up-sell existing customers with upgrades, new features, or value-added services that can be electronically activated; target emerging customer needs or preferences without the need to sell or exchange new hardware; offer flexible pricing or subscription models that tailor capabilities and services to specific customers; and utilize transactional information and other data to improve services.

However, in order to take advantage of this financially lucrative but rapidly evolving market, companies will first need to assert valid ownership rights in the relevant intellectual property covered by the software or technology license. Unfortunately, because of the nature of the IoT, businesses may face some unique challenges when seeking to enforce their patents and claim exclusive rights in the device’s underlying technology. In particular, the Supreme Court’s recent decision in Alice Corp. v. CLS Bank has further clouded the already unsettled issue of when and to what extent computer programs are patent-eligible. In Alice, the Court hardened the rules for determining which inventions are eligible to be patented. Under the U.S. Patent Act, “any new and useful process, machine, manufacture, or composition of matter, or any new and

useful improvement thereof, may be eligible for patent protection.”\textsuperscript{201} However, U.S. courts have developed three exclusions to this broad provision: laws of nature, natural phenomena, and abstract ideas are considered patent-ineligible subject matter. According to the Supreme Court in Alice, an invention that uses or relies on ineligible subject matter, like abstract ideas, can only qualify for a patent if the remaining parts of the invention have some sort of “inventive concept” that transform the ineligible claim into a patent-eligible application.\textsuperscript{202} In Alice, the invention was a computerized method configured to perform electronic escrow for online transactions.\textsuperscript{203} The Court found the patent on this invention claimed an abstract idea (escrow), which was patent-ineligible.\textsuperscript{204} The remainder of the invention—performing the escrow on a general purpose computer—was not sufficient to provide an inventive concept. According to the Court, “a mere instruction to implement an abstract idea on […] a computer […] cannot impart patent eligibility.”\textsuperscript{205}

Although the Supreme Court did not specifically rule on the patentability of software or business methods, the opinion had a profound impact on the patent eligibility of computer-implemented inventions. In fact, since the decision in Alice was rendered, courts have invalidated the vast majority of software patents and business-method patents on the basis of the Supreme Court’s guidance, reasoning that these patents lacked an “inventive concept” that took them beyond “ineligible abstract ideas.”\textsuperscript{206} Instead, as one district court recently opined, such patents, while “frequently dressed up in the argot of invention, simply describe a problem, announce purely functional steps that purport to solve the problem, and recite standard computer operations to perform some of those steps.”\textsuperscript{207} Likewise, following Alice, the U.S. Patent and Trademark Office issued new guidelines for its examiners, imposing greater scrutiny on business methods and inventions related to software.\textsuperscript{208} Using these guidelines, the PTO has struck down software and business-method patents in record numbers and denied

\begin{itemize}
\item 202. Alice, 134 S.Ct. at 2355.
\item 203. Id. at 2349.
\item 204. Id. at 2355.
\item 205. Id. at 2358; see also Steven Seidenberg, Business-Method and Software Patents May Go Through the Looking Glass After Alice Decision, ABA JOURNAL (Feb. 1, 2015, 2:40 AM), http://www.abajournal.com/magazine/article/business_method_and_software_patents_may_go_through_the_looking_glass_after.
\end{itemize}
applications that previously would have been accepted. These developments not only deprive software-related inventions of necessary patent protection, they also tilt the playing field in favor of accused infringers, who can simply argue that the issued patent is ineligible. According to one researcher who has analyzed court and PTO decisions post-*Alice*: “we will continue to see the zone of patent eligibility curtailed in software.” Indeed, the more advanced the software technology—the more it takes over the cognitive work once done exclusively by humans, the more seamless it becomes in the fabric of our daily lives—the less patent eligible it is deemed to be by the courts and the USPTO.

Another crucial problem for companies involved in IoT technology is the issue of “divided infringement.” In order to be liable for infringement of what is known as a “method” patent claim (a series of acts or steps for accomplishing a result), a single person (infringer) must perform each and every step of that patented claim. Alternatively, a party could be liable for “induced infringement” by aiding or abetting another in infringing a patent. But what if multiple parties collectively perform all of the steps of a claimed method? This scenario, known as “divided infringement,” could conceivably arise with any technology that requires interaction between multiple parties or multiple components. According to a recent Supreme Court decision, there must be a single actor performing all of the elements of a patentable claim before a party can be held liable for infringement. As mentioned earlier, however, IoT technology typically requires the involvement of multiple stakeholders in the design, manufacture, and operation of Internet-connected devices. This will inevitably lead to a situation where each step of an IoT company’s method claim could be (or must be) performed by different parties, none of whom have any control over the others. In such a situation, if there is no single party performing each of the elements of the patented claim, then no one can be held liable for infringement. As a result, there are serious questions about whether IoT patent claims that are typically practiced by multiple actors can even be enforced.

IoT businesses should continue to monitor this area of the law closely. To the extent possible, when drafting a patent method claim, companies should focus on steps or acts that can be performed by a single actor; those claims that require multiple actors may be difficult to enforce against alleged infringers.

212. *Id.*
214. *Id.* at 4.
215. *Id.* at 4.
216. *Id.* at 7.
Moreover, with the patentability of software inventions in serious doubt, IoT companies will need to be selective with their patent strategy and should consider whether any patent claims that can be obtained will be broad enough to warrant the time and expense associated with patent prosecution.\footnote{219}{Software Patents, \textit{IPWATCHDOG}, \texttt{http://www.ipwatchdog.com/software-patents/} (last updated May 27, 2014).}

\textbf{E. Data Ownership}

As previously discussed, the true value of the IoT for businesses is in gaining access to and analyzing the massive data streams contained in embedded technology. But who actually owns or has rights in this data? Unlike a typical IP claim where the merchant asserting a legal interest in the data is responsible for its creation, here, all of the data that is tracked or collected is generated by the end-user, which is often a consumer.\footnote{220}{Lars Smith, \textit{Rfid and Other Embedded Technologies: Who Owns the Data?}, 22 SANTA CLARA COMPUTER & HIGH TECH. L.J. 695, 755 (2006).} Further, in contrast to situations where the party claiming proprietary rights in the data owns the hardware where data is stored, IoT data is contained in objects or devices that are the personal property of the consumer.\footnote{221}{\textit{Id.} at 738–39, 755.} Under Article 2 of the UCC, if the transaction is a sale of goods, then title to the entire good transfers to the consumer, whether or not the seller tries to retain title to part of the good through a contract provision (in this case the computer chip embedded in the object).\footnote{222}{\textit{Id.} (citing U.C.C. §§ 2-101–2-725 (as amended 2002) & U.C.C §§ 9-101–9-725 (as amended 2013)).} As a result, the consumer owns the physical media where the data is stored. The UCC is silent, however, about whether ownership of the good includes ownership of the data contained in that good.\footnote{223}{\textit{Id.} at 711 (citing Feist Publications, Inc. v. Rural Tel. Serv., 499 U.S. 340, 347–48 (1991)).}

While a \textit{compilation} of data can be copyrightable, a business attempting to protect a database with a copyright would need to show that the data it tracked was selected, coordinated, or arranged in an \textit{original} fashion.\footnote{224}{Smith, \textit{supra} note 220, at 712–15.} Yet, because data collected by IoT sensors is often compiled automatically through a standard set of selection criteria rather than any human involvement, it could be difficult to establish a valid copyright in many IoT-related data compilations.\footnote{225}{Smith, \textit{supra} note 220, at 715–16.} Even if a compilation were copyrightable, a single data point within that compilation would not be subject to copyright protection.\footnote{226}{\textit{Id.} at 741–42.}

It could be possible for IoT companies to claim that trade-secret law protects the data tracked by IoT devices. A trade secret can be any information that gives an owner a competitive advantage. Under a trade secret claim, the database

---


\textsuperscript{221} \textit{Id.} at 738–39, 755.

\textsuperscript{222} \textit{Id.} (citing U.C.C. §§ 2-101–2-725 (as amended 2002) & U.C.C §§ 9-101–9-725 (as amended 2013)).

\textsuperscript{223} \textit{Id.} at 741–42.

\textsuperscript{224} \textit{Id.} at 711 (citing Feist Publications, Inc. v. Rural Tel. Serv., 499 U.S. 340, 347–48 (1991)).

\textsuperscript{225} Smith, \textit{supra} note 220, at 712–15.

\textsuperscript{226} \textit{Id.} at 715–16.
owner generally needs to prove that: (1) the data is secret, (2) its value is derived from its secrecy, and (3) the owner used reasonable efforts to safeguard its secrecy or limit access to the data. However, in the typical trade-secret case, the records claimed to be trade secrets are created by the owner or its employees and stored in the owner’s own computer system; here, in contrast, the end-user or consumer is the creator of the data and the likely owner of the hardware where the data is stored. Conceivably, then, if it is the consumer that owns the data, he or she is free to determine how to use that data, including whether to keep the data confidential. It is thus unclear in this scenario whether a court would be willing to protect the data contained in an IoT device as a trade secret. With the continued uncertainty over which parties own or have proprietary rights in this valuable data, companies should, at the very least, seek to ensure that their licenses and end-user agreements are clear with respect to data ownership and use rights.

Businesses can also use password protection, encryption, or other technological measures designed to prevent unauthorized access to the data residing in the IoT device. The Digital Millennium Copyright Act prohibits people from circumventing technological measures that control access to a copyrighted work, although there is considerable uncertainty whether IoT databases can be copyrightable. Licenses and end-user agreements would thus likely include strict restrictions on circumvention, reverse-engineering, and even unauthorized repair services. Once again, companies will also need to consider how to bind multiple end-users, including future users who have purchased the product on the secondary market, to such restrictions.

Yet, the above discussion on merchant vs. consumer ownership of IoT data says nothing about which merchant along the data processing chain can assert valid ownership of such data. As noted earlier, there are a number of stakeholders involved in the IoT ecosystem, including device manufacturers, application developers, data platforms, device lenders, social media platforms, data brokers, cloud service providers, and any third-party purchasers of the data, among others. Given the multitude of actors that have access to, or otherwise process the data emitted from an IoT device during the product’s lifecycle, and the nature of device-to-device data sharing and processing, legal disputes will inevitably arise over which entity has the exclusive ownership rights to commercially exploit that data, particularly when contractual arrangements fail to properly allocate rights and responsibilities along the data chain.

F. Data Storage and Management

228. Smith, supra note 220, at 725.
The IoT will produce an explosion of data that can be leveraged to trigger new revenue streams, novel business models, and improved business intelligence, among other things. But how will IoT businesses manage the flood of continuous data streams that need to be processed and analyzed in real time? According to a recent survey, more than half of 400 IT chiefs indicated that their companies’ networks were already at full capacity and would struggle to cope with any additional workload. With the growing number of IoT devices, as well as the unrelenting flow of inbound IoT data, enterprises will face enormous challenges and costs processing, storing, securing, and managing those assets in a single location. While many companies have centralized their data centers to reduce costs and tighten security, most companies will not have the infrastructure scalability—including bandwidth, disk storage, and processing power—to keep up with the demand for data ingestion, storage, and real-time analytics, while also remaining compliant with their data protection obligations. As the IoT continues to grow, enterprises will increasingly shift toward outsourcing these responsibilities to cloud service providers. Yet, ceding custody—and to some extent management—of sensitive and/or proprietary data to a third party raises a litany of new legal obligations and risks. In particular, in the absence of favorable contractual terms, responsibility for any privacy violations or security breaches will remain with the contracting company, even if actual fault lies with the cloud service provider. Issues surrounding privacy governance and the cloud remain unsettled in most jurisdictions; IoT enterprises that outsource data processing responsibilities to the cloud will thus need to carefully consider each party’s respective legal obligations and monitor how those obligations may evolve over time.

G. Extraterritorial Jurisdiction

Because connected IoT devices will physically cross borders along with their end-users, they will inevitably implicate the laws of multiple jurisdictions, many of which may be more restrictive than the data protection laws found in the U.S. Under Directive 95/46/EC—the European Union’s current data protection framework that requires EU Member States to promulgate their own omnibus data protection law modeled off the Directive itself—EU member states’ national data protection laws apply to all processing of personal data where an operator

---


uses “equipment” situated on a member state’s territory. According to the Article 29 Working Party, which is composed of representatives of the data protection authorities from each EU Member State, all objects that collect and process individuals’ data while providing IoT services are considered “equipment” under the Directive.\textsuperscript{233} As a result, IoT companies operating outside the EU may still be subject to EU data protection laws if individuals that are located in the EU use any of its IoT devices. For example, a company that sells smart watches, and is exclusively based in the U.S., will be subject to the data protection laws of an EU Member State whenever one of its watches collects and processes data within that country. Likewise, IoT companies that rely on cloud service providers for their infrastructure and data processing needs will need to account for both the jurisdictional exposure of their own operations as well as the jurisdictional reach of their cloud providers, many of whom move data seamlessly from country to country.

Moreover, the proposed EU General Data Protection Regulation (“GDPR”)\textsuperscript{234}—which seeks to harmonize EU data protection laws by replacing Directive 95/46/EC and instituting a single set of binding rules applicable to all EU member states—would significantly expand the already broad extraterritorial reach of EU data protection laws.\textsuperscript{235} Article 3(2) of the draft GDPR extends the application of EU law to the processing of personal data by a data controller not established in the EU where the processing activities are related to: (1) the offering of goods or services to data subjects in the EU, irrespective of whether payment is required or (2) the monitoring of their behavior.\textsuperscript{236} In other words, with respect to companies not based in the EU, the GDPR essentially changes the focus from the Directive’s “use of equipment” test to non-EU entities that offer goods and services to, or monitor the behavior of, EU data subjects. Consequently, the GDPR’s proposed jurisdictional scope threatens universal application of EU data protection laws to the entire Internet.\textsuperscript{237} For example, the mere placement of a cookie on an EU data subject’s device would place the operator of that tracking technology under the ambit of EU law. Under the GDPR, “companies with little or no geographical nexus to the EU are effectively expected to modify their entire business models and establish elaborate internal governance schedules (including data protection officers, data protection impact

\textsuperscript{233} \textit{EU IoT Report, supra} note 47, at 10.


\textsuperscript{236} Id.

\textsuperscript{237} Id. at 3.
assessments, restrictions on international data transfers, and more) to comply with EU law.  

Many of these legal requirements will raise a particularly significant compliance burden for IoT entities. The “right to data portability,” under Article 18 of the proposed GDPR, for example, gives data-subjects the right to receive from data controllers their personal data in a commonly used electronic and structured format that allows for further use by other data controllers. Yet, this requirement assumes a certain level of interoperability that is currently not present among horizontal IoT platforms. If the IoT ecosystem continues to develop as a walled garden of proprietary technology and closed systems, how can IoT operators assure this kind of data portability in compliance with the GDPR?

Perhaps more troubling for IoT organizations is the GDPR’s “Right to Be Forgotten” (or, more precisely, the right to erasure) under Article 17, which requires data controllers to erase personal data when, among other things: (1) the data is no longer necessary for the purpose it was originally collected or (2) the data-subject objects to the processing of the data and there are no overriding legitimate grounds for processing. As noted earlier, the true value of IoT devices to businesses is the massive amounts of insightful data they collect. Companies cannot predict (and thus cannot communicate to data subjects at the time of collection) all of the potentially valuable ways they may use the data they collect in the future. However, under the GDPR, even if IoT companies think of new ways to use the data that are not otherwise harmful or intrusive to individual privacy, they will still be required to erase that data if it is no longer necessary for the stated purpose in which it was originally collected.

Moreover, if the number of connected devices already outnumber humans, and those devices are constantly switching hands among end-users, it may be unrealistic to expect IoT organizations to maintain the level of internal oversight and control necessary to effectively manage data flows and data usage for each device in the wild. Yet, the costs of non-compliance could be crippling: under the GDPR, penalties could reach €20 million or 4% of a company’s annual global turnover (total revenues), whichever is higher.

In sum, privacy regimes that focus on the location of data processing activities or data subjects for determining when to exercise jurisdiction over an organization are increasingly coming into conflict with the globalized and porous nature of connected devices and big data. The broad extraterritorial reach of many privacy laws—most notably the EU’s data protection regime and data localization requirements in Russia and other jurisdictions—could subject IoT

238. Id.
239. See GDPR, supra note 234, at 110.
240. Id. at 107–09.
241. Id. at 107.
242. Id. at 196–99.
companies to foreign law irrespective of whether they have a physical or legal presence in that particular jurisdiction. As a result, companies must ensure compliance with applicable legal obligations imposed by other jurisdictions, many of which may be more restrictive than, or in direct conflict with, their domestic laws. To make matters more complicated, because intellectual property rights are typically territorial in nature, any IP rights an IoT company possesses in software or data will vary from country to country. Companies will thus need to consider whether the benefits of the IoT outweigh the costs and risks of navigating the potential labyrinth of legal rights and responsibilities.

VII. CONCLUSION

Despite the IoT’s potentially groundbreaking economic potential, the cutting edge legal and regulatory issues that it raises means that the path forward is far from clear. Although U.S. regulatory agencies are beginning to recognize the growing impact of the IoT, no new federal laws or regulations governing the IoT are expected in the near future. While state legislatures may attempt to fill the gap, such a piecemeal approach will continue to create compliance headaches for companies that are continuously processing data across borders.

Nonetheless, it is clear that, as the IoT exponentially multiplies the amount of useful data available, it will increasingly become a serious topic of focus among legislative, regulatory, and self-regulatory bodies. The FTC will continue to be the most active regulator in this sphere: in addition to releasing its 2015 report on the IoT, the FTC’s Commissioner has communicated the need for the FTC to use its enforcement authority to monitor any privacy, data security, and general consumer protection harms that may arise from the development of IoT devices. The FTC typically regulates privacy and cybersecurity under its “deception” authority, bringing claims that companies deceived consumers by misrepresenting their privacy or data security practices in their public statements. However, in TRENDnet—the agency’s first and only enforcement action against an IoT company—the FTC went beyond the standard misrepresentation claim. Citing its authority to regulate unfair trade acts or practices, the agency charged that TRENDnet failed to: (1) implement reasonable security measures by storing and transmitting user login credentials in “clear, readable text” rather than using “free” software to encrypt consumer data; (2) monitor security vulnerability reports from third parties; (3) test and review potential security vulnerabilities in its software; and (4) implement “reasonable guidance or training” for

244. Several U.S. regulatory agencies are currently researching the privacy and cybersecurity implications of the IoT, and members of the Senate Commerce Committee recently requested an oversight hearing regarding the novel questions surrounding IoT related to consumer protection, privacy, security, and manufacturing.
245. Ohlhausen, supra note 2.
employees. Among other things, TRENDnet’s settlement with the FTC required it to implement a comprehensive information security program and submit to biennial third-party assessments of its security program for 20 years.

At the same time, with a tightened budget and a continued emphasis on traditional privacy tools like notice and consent that are arguably ill-suited for the emerging IoT, the FTC may be limited in its ability to keep up with technological innovation while safeguarding consumer privacy and security in a way that does not disadvantage businesses and obstruct IoT development. The IoT wave could fundamentally change the way enterprises do business while triggering unique revenue generating possibilities for those that can capitalize on its opportunities. As always, however, the law will struggle to keep pace with technological advancements. While the potential benefits are clear, the IoT’s promise will ultimately depend on whether the current legal landscape evolves in ways that foster innovation and growth, rather than stifling it. The legal issues and risks companies face will, in turn, be shaped by what the IoT eventually becomes: from a global open system that interfaces with everything, to myriad closed networks that accomplish discrete purposes, to something in between.

246. Complaint, supra note 107.
247. Id.
HIDDEN THREAT: THE DARK WEB SURROUNDING CYBER SECURITY

A. Dominick Romeo*

I. INTRODUCTION

Every time you access the Internet you take a huge risk. This is a troubling proposition because almost every facet of American life involves accessing the Internet. Whether it’s financial transactions, social interactions, academic research, or something in-between, there isn’t an aspect of our collective lives not connected to the Internet. Even commerce is now dominant online, thanks to retailers like Amazon. With the amount of personal information exchanged online everyday, it should come as no surprise that a threat exists in cyberspace; our personal information is vulnerable as cyber-criminals become more cunning and authorities fall behind.

In recent years, cyber security has spawned a hotbed of issues—ranging from privacy to national security. In light of the increasing rate of data breaches, there is an argument that the state of American cyber security is uncertain at best. Take, for example, the most recent high-profile data breach, where a hacker stole 22.1 million federal employees’ security files. Officials consider the information obtained in that breach as “a treasure trove of information about anyone who has worked for . . . or currently works for the United States

* I would like to thank Brooke McCloud, Tuck Romeo, and Boone Romeo.
1. U.S. CENSUS BUREAU, MEASURING AMERICA: COMPUTER AND INTERNET TRENDS IN AMERICA (2014), https://www.census.gov/hhes/computer/files/2012/Computer_Use_Infographic_FINAL.pdf (showing that computers are in eighty percent of homes and approximately ninety-five percent of them are used for internet access).
3. Id.
4. See infra notes 7–10.
6. See INFO. SYS. AUDIT AND CONTROL ASS’N, STATE OF CYBERSECURITY: IMPLICATIONS FOR 2016, 2 (2016), http://www.isaca.org/cyber/Documents/state-of-cybersecurity_res_eng_0316.pdf (“The current state of global cybersecurity remains chaotic, the attacks are not expected to slow down, and almost 75 percent of respondents expect to fall prey to a cyberattack in 2016.”).
government.” The Rand group, a research organization that develops solutions to public policy challenges to help make communities throughout the world more safe and secure, estimated in a June 2015 report that cyber security spending will increase thirty-eight percent through 2025. Even with this large increase, some chief information security officers believe that no amount of spending will mitigate the trends that experts are currently tracking. Which then begs the critical question: as cyber criminals are honing their skills and launching increasingly sophisticated attacks, will we ever truly be cyber secure? Or alternatively, how much risk are we willing to accept as our lives increasingly depend on the Internet?

II. THE DEEP WEB AND THE DARK WEB: THE SOURCE OF THE PROBLEM

While cyber crime is prevalent in the news lately, there is little discussion about the roles that the “Deep Web” and “Dark Web” play in fueling cyber crime, and how they run counter to defending the current cyber security infrastructure. It wasn’t until the Silk Road prosecution that the American people got a true glimpse of the Dark Web’s contents and potential. Most Americans are now aware that Silk Road was an online marketplace specializing in the exchange of illegal goods, primarily narcotics. But most people do not know that the Dark Web, the platform through which Silk Road operated, poses the greatest threat to cyber and national security. To understand the risk that the Dark Web poses, one must first understand how it works.

A. SURFACE WEB, DEEP WEB, AND DARK WEB

There are essentially three layers of the Internet. First, there is the Surface Web, which is used by everyone who browses the Internet. The Surface Web is

8. Id. (stating that information obtained by the hackers contained social security numbers and information related to job interviews and assignments).
10. Chris Dimarco, The Dark Web: A Look into the Cybercriminal Underworld, L. TECH. NEWS, June 19, 2015, LEXIS.
11. Id. (showing that the same RAND report states that CIO’s do not believe the additional investment will be enough to combat the faculties at the disposal of increasingly sophisticated attack behaviors and threats).
13. See Burleigh, supra note 12.
anything that a standard search engine can find. It includes the typical search engines and all indexed websites, e.g., Google, Facebook, and Yahoo.17

The Deep Web “is anything that a search engine cannot find.”18 But that doesn’t mean that casual Internet users don’t use the Deep Web. As one blog notes, “[e]xamples of Deep Web content can be found almost anytime you navigate away from Google and do a search directly in a website.”19 In fact, what you find after searching your local court docket online is part of the Deep Web.20 More generally, the Deep Web is home to academic library databases, proprietary databases, and results of database queries,21 as well as things like user databases, webmail pages, registration-required web forums, and pages behind paywalls, which are basically pages that search engines cannot connect directly to because they are user-specific and require passwords—Westlaw, for example.22 The sheer scale of the Deep Web is almost incomprehensible.23 It is estimated that public information available on the Deep Web is 1,000 to 5,000 times greater than public information on the Surface Web.24

Finally, there is the Deep Web’s seedy underbelly, the Dark Web. It is “classification as a small portion of the Deep Web that has been intentionally hidden.”25 The Dark Web cannot be accessed through standard web browsers.26 It can only be accessed through specialized tools or interfaces, the most popular of which is the Tor network.27

Brownlee, The Deep Web and the Dark Web—An Overview for Lawyers, INTELL. PROP. DUE DILIGENCE IN CORP. TRANSACTIONS, Apr. 2016, § B.1:2. The Author encourages all who have trouble conceptualizing the difference between the Surface Web, Deep Web, and Dark Web to take a look at these articles.

16. Id.
17. See id.
18. Id.
19. Id.
20. See id. (noting that government databases and libraries contain huge amounts of Deep Web data and including an online court database as an example.).
23. See Jose Palgiery, The Deep Web You Don’t Know About, CNN MONEY (Mar. 10, 2014, 9:18 AM), http://money.cnn.com/2014/03/10/technology/deep-web/index.html (stating that the best and most current estimates speculate that the web we know—Facebook, Twitter, and Google, for example—make up less than 1% of the entire World Wide Web).
26. Id.
27. Id.; see also Swift, supra note 12 (stating that Tor is software that routes your web
Tor is special software that anyone can download for free. It allows users to browse the web with anonymity. The U.S. Naval Research Laboratory developed the Tor browser in the mid 1990’s to: (1) protect online communications among military and governmental agencies and (2) facilitate “open-source intelligence gathering.” Tor allows users to send and receive messages and remain anonymous through a process known as “onion routing.”

Tor software routes a user’s web traffic through a “worldwide volunteer network of servers” rather than making a direct connection, which allows a user to prevent websites from tracking them and to share information over public networks without compromising privacy.

Anonymous browsing has beneficial applications; people in repressed countries have used Tor to circumvent government censorship and avoid persecution for online activities. Moreover, the Tor network has become instrumental for whistleblowers who wish to disclose valuable information without compromising their identity. In this respect, the Tor network is an invaluable tool in the cyber age; it is a way for people to exchange information anonymously in ways they never could before.

Despite the benefits of Tor and the Dark Web, they still remain the greatest threats to cyber security. If it wasn’t for the Silk Road case, it is doubtful that the general public would even be aware of the dangers of the Dark Web. Most connections through a number of other web servers—possibly around the world – in order to hide the source and destination of the connection).

28. Id.; see also Tor Project Overview, TORPROJECT.ORG, https://www.torproject.org/about/overview.html.en (last visited Apr. 5, 2016).


31. Natasha Bertrand, ISIS is Taking Full Advantage of the Darkest Corners of the Internet, BUS. INSIDER (July 11, 2015, 11:26 AM), http://www.businessinsider.com/isis-is-using-the-dark-web-2015-7 (explaining that “[j]ust as an onion has multiple layers, onion rooting on Tor protects people’s identities by wrapping layers around their communications’ that are impenetrable—and thereby untraceable—by either party . . . .”); Chertoff & Simon, supra note 29, at 4.

32. Chertoff & Simon, supra note 29, at 3.


34. Ingmar Zahorsky, Tor, Anonymity, and the Arab Spring: An Interview with Jacob Appelbaum, U. FOR PEACE AND CONFLICT MONITOR (July 29, 2015), http://www.monitorforpeace.org/innerpg.cfm?id_article=816 (explaining that during the Arab Spring bloggers, journalists, and online activist utilized the Tor network in order to circumvent government censorship of certain social media websites and bring news of the then uprising against autocratic presidency of Hosni Mubarak).

35. Chertoff & Simon, supra note 29, at 5 (noting that whistleblowers, human rights workers struggling against repressive governments, and parents trying to create a safe way for their children to explore the web are a few useful examples of the application of Tor).
people assume the Dark Web is a hidden entity shrouded in secrecy, only accessible to the most-skilled hackers. But that’s not the case.36 The Dark Web is more accessible than people care to believe.37 And the frightening reality is that any person with an Internet connection can access the Dark Web.38

B. Dark Web Marketplaces and Their Currency

1. What’s For Sale?

Now that we have a basic understanding of how the Dark Web works on a technical level, let’s explore the environment that anonymous browsing and the Dark Web have fostered. The Dark Web spurred the creation of a vast online black market; there are a myriad of illicit items bought and sold on it everyday.39 Examples of what’s available on the Dark Web include, but are certainly not limited to:

- Firearms;40
- Passports;41
- Drivers licenses and ID cards;42
- Healthcare data, which includes intimate patient information;43

36. Brownlee, supra note 15, § B.1:10 (positing that the entire process of installing and using Tor takes less than 30 minutes).
38. Id.
41. Investigations have revealed that there are sellers advertising themselves as insiders who can create genuine passports with an entirely new set of credentials provided by the buyer. Alistair Charlton, Dark Web Vendors Sell Blank British Passports and Entry to Passport Databases for Just £2,000, INT’L. BUS. TIMES U.K. (July 7, 2015, 15:31 BST), http://www.ibtimes.co.uk/dark-web-vendors-sell-blank-british-passports-entry-passport-database-just-2000-1509564. Moreover, it was also disclosed to the undercover journalist that the passports could come with “visa stamps to add to their legitimacy.” Id. Indeed, this undercover investigation found sellers of blank passports in England, Canada, and Germany. Id.
42. Id.
43. See Mark Lanterman, Not What the Doctor Ordered: Security Concerns in Light of Evolving Health Technologies; Health Care Professionals Must Stay Current on How Best to Protect Data Breaches, 17 NO. 4 J. HEALTH CARE COMPLIANCE 5, 8 (July–Aug. 2015). In fact, the price for healthcare data fetches more than credit card information because of the relatively high profits of healthcare fraud. Id.
• Credit card and Social Security numbers;\textsuperscript{44} and
• Child pornography and other child abuse material.\textsuperscript{45}

2. How Are Things Paid For?

The growth of Dark Web marketplaces is fueled by the use of digital crypto-
currencies like Bitcoin.\textsuperscript{46} Bitcoin is the most widely used currency in Dark Web
transactions.\textsuperscript{47} It is unique in that it is a completely self-sufficient currency that
is backed by no country or national bank.\textsuperscript{48} It is instrumental in Dark Web
marketplaces because it allows users and transactions to remain completely
anonymous.\textsuperscript{49} Indeed, the use of Bitcoin makes it almost impossible for a
purchaser or seller to know where the currency is being transferred.\textsuperscript{50}

3. Can We Regulate Bitcoin?

Bitcoin has a promising future as a viable medium of exchange for the online
world, but it is subject to the same security concerns that personal databases are
vulnerable to.\textsuperscript{51} Only when Bitcoin is effectively regulated will the criminals
operating on the Dark Web cease to prosper.

Thus, we are forced to consider how Bitcoin can be regulated to prevent
illegal uses. The current approach is through the use of extreme sentencing
measures, i.e., Ross Ulbricht’s (the founder of Silk Road) life sentence will deter
others from operating a sophisticated black market bazaar.\textsuperscript{52} However, we know
that is not the case, as Silk Road 2.0 quickly filled the void.\textsuperscript{53} As another article
notes, “[a]s much as $8 million in transactions occurred on Silk Road 2.0, which
was hardly the largest deep web commerce site.”\textsuperscript{54}

\textsuperscript{44} Chertoff & Simon, supra note 29, at 4; Reisinger, supra note 40.
\textsuperscript{45} Chertoff & Simon, supra note 29, at 5.
\textsuperscript{46} See Assistant Attorney General Leslie R. Caldwell Delivers Remarks at the ABA’S National
Institute on Bitcoin and Other Digital Currencies, U.S. DEP’T OF JUSTICE (June 26, 2015),
\textsuperscript{47} Id.
\textsuperscript{48} Catherine Martin Christopher, Whack-A-Mile: Why Prosecuting Digital Currency
\textsuperscript{49} Id. at 14 (explaining that in order to send or receive Bitcoin, one must have a Bitcoin
address; a Bitcoin address is like an e-mail address but it is merely a string of numbers and contains
no identifying information about the account owner).
\textsuperscript{50} Id.
\textsuperscript{51} Id. at 21 (noting that a hacking attack on Mt. Gox, a Bitcoin exchange, in 2011 resulted in
the theft of 25,000 Bitcoin, valued at $8.75 million).
\textsuperscript{52} Remarks of Leslie Caldwell, supra note 45.
\textsuperscript{53} See Zagaris, supra note 30.
\textsuperscript{54} Aaron DeVera, A Beginner’s Guide to Buying Drugs and Guns on the Web, FORDHAM POL.
Alternatively, it is suggested that industry regulators must take an active role in the policing and regulating digital currencies like Bitcoin. The current trend is to rely on money services business, money transmission statutes, and anti-money laundering statutes when prosecuting crimes originating on the Dark Web. However, this largely fails to address the needs and importance of comprehensive online currency regulation. And further, no current legislation is aimed at curbing Dark Web activity.

Moreover, it is important to note that digital currencies like Bitcoin, in their current state, cannot be regulated. Only the transactions and the third parties facilitating those transactions can be regulated. The most promising form of regulation would be stricter Financial Crimes Enforcement Network (“FinCEN”) compliance. In March 2013, FinCEN announced that it would begin applying anti-money laundering statutes to digital currencies. Failure to register with FinCEN as a money service business will now result in an investigation and overhaul of anyone conducting business with Bitcoin. But the critical issue lies in the fact that Bitcoin itself can never be shut down as it operates on a P2P network. Bitcoin operates simultaneously on a multitude of personal computers, is open source, visible to anyone who looks for it, and is free—effectively shielding it from law enforcement.

C. The Greater Dangers Promoted by the Dark Web

1. A Tool for Terrorists

With all this in mind, it is easy to recognize that the Dark Web is a vital tool for terrorist organizations like ISIS. Unfortunately, however, the danger doesn’t end with what terrorist organizations can purchase on the Dark Web. The Dark Web also allows for members of terrorist organizations to communicate online anonymously. Terrorists groups traditionally relied on

55. Remarks of Leslie Caldwell, supra note 45.
56. Id.
57. Id. (The State of New York has established virtual-currency specific licensing requirements).
58. Christopher, supra note 47, at 22.
59. Id. at 23.
61. Christopher, supra note 47, at 23.
62. Remarks of Leslie Caldwell, supra note 45 (RippleLabs was a merchant of a virtual currency called XRP and failed to comply with FinCEN’s anti-money laundering protections).
63. Christopher, supra note 47, at 28.
64. Id.
65. See Bertrand, supra note 31; see also Chertoff & Simon, supra note 29, at 5 (stating that “dark [w]eb and terrorists seem to compliment each other — the latter need an anonymous network that is readily available yet generally inaccessible.”).
66. See Bertrand, supra note 31.
surface websites to drum up recruitment and spread propaganda. But, in an
effort to remain anonymous, sympathizers and militants have begun utilizing the
Dark Web. Indeed, different authorities have noted that the recent shutdown of
radical websites on the Surface Web has forced jihadists into the Dark Web
where they cannot be monitored or tracked.

In addition to recruitment and communications, terrorists groups are now
using the Dark Web to solicit financing for global operations away from the
prying eyes of intelligence officials and law enforcement. For example, in July
2015, ISIS supporters posted informational pages instructing sympathizers on
how to use the Dark Web to donate money anonymously.

2. The Dark Web’s Cyber-Security Threat

There is a burgeoning market for credit card and healthcare information on
the Dark Web. And the emergence of an economy for stolen information means
that criminals operating on the Dark Web are sufficiently financed by other
criminal organizations. Indeed, the number one reason that data breach attacks
have become so prevalent today is because of the high value of personal
information.

Likewise, the reality is that cyber security threats are primarily driven by the
prospect of financial gain. IBM Executive Security Advisor Diana Kelly has
claimed that “the main driver behind attacks . . . is the increasing value of the
information and access that hackers can steal then sell for profit on the dark
web.” Furthermore, Kelly opined that criminal hackers are forming complex
organized crime rings and coordinating attacks together in an effort to maximize
the devastation. The American people know that organized crime rings can be
capable of wreaking havoc; the issue was all too prevalent in the early twentieth
century because bootleggers and mobsters had more powerful weapons and faster

67. Id.
68. Id. (quoting Aamir Lakhani, senior security strategist at Fortinet, who told Business Insider
that the “dark web has become ISIS’s number one recruiting platform . . . ”).
69. Id.; Tom Whitehead, Terrorist Material Reappears Online ‘As Quickly As it is Banished,’
Warns Think Tank, THE TELEGRAPH (Dec. 24, 2014, 10:00 PM GMT),
http://www.telegraph.co.uk/news/uknews/terrorism-in-the-uk/11300881/Terrorist-material-
reappears-online-as-quickly-as-it-is-banished-warns-thinktank.html (“Attempts to block extremist
material online will always fail despite a British counter-terrorism unit taking down more than 100
web pages a day, a think tank has warned.”).
70. Id.
71. Id. (dark wallet is a “dark web app that promises to keep users Bitcoin transactions
anonymous”).
72. Taylor Armerding, Dark Web: An Ever-More-Comfortable Haven for Cyber Criminals,
CSO (Mar. 28, 2014, 8:10 AM PT), http://www.csoonline.com/article/2137223/data-
73. See Dimarco, supra note 10.
74. See id.
75. Id.
76. Id.
cars than law enforcement officials. Similarly, cyber criminals today, are becoming more sophisticated and organized, leaving law enforcement in the dust.

Consider, for example, the Anthem Insurance breach, one of the largest healthcare breaches to date.77 The hackers breached a database containing the records of millions of current and former Anthem customers.78 Unlike past healthcare breaches, this breach took months of planning and resulted in the acquisition of high-level employee credentials.79 And, given what we know about the market for this information on Dark Web exchanges, the hackers were probably able to sell it for a huge profit.80

Nevertheless, state-sponsored cyber warfare is increasingly prevalent in today’s world.81 Though traditional targets—governmental agencies and research institutions—are no longer primary targets. Instead, state-sponsored cyber attacks are focusing on the economies of rival nations.82 In 2014, a Chinese group was blamed for attacks on U.S. aerospace and communications companies.83 More recently, Sony was the victim of malicious cyber attack conducted by Guardians of the Peace, a group with ties to the North Korean Government.84

Overall, the Dark Web poses a serious risk to national and domestic cyber security as demonstrated by several high-profile cases.85 Efforts to strengthen cyber security, however, can be undone as a result of something as simple as human error.86 Governments and private industries need to take careful measures when they store sensitive information in an online database. Otherwise, even “good technical security measures” run the risk of being “ineffective because of lapses with the human element of security.”87

77. See, e.g., Lanterman, supra note 43, at 8.
78. Reed Abelson & Matthew Goldstein, Millions of Anthem Customers Targeted in Cyberattack, N.Y. TIMES (Feb. 5, 2015), http://www.nytimes.com/2015/02/05/business/hackers-breached-data-of-millions-insurer-says.html?_r=0 (“The information accessed included names, Social security numbers, birthdays, addresses, email and employment information, including income data.”).
80. See supra text accompanying note 43.
82. See id.
83. Id. at 2.
84. Id. (stating that the attack on Sony “resulted in the loss of personal information of employees and their families and the exposure of executive-level salaries and company email exchanges”).
86. See, e.g., Lanterman, supra note 43, at 9 (where Target had good security measures, but allowed an outside vendor to connect to the same network responsible for point-of-sale device, thus opening up customer date vulnerabilities).
87. Id.
III. RECENT SUCCESSES: HOPEFUL PROSPECT OR FALSE OPTIMISM?

In April 2015, the United States government and various other agencies seized and shut down an alleged Uganda-based counterfeiting scheme operating on the Dark Web.88 Law enforcement infiltrated the foreign counterfeiting ring that openly advertised and sold counterfeit Federal Reserve Notes on the Community-X Dark Web page.89 But even after the shutdown of sites like the aforementioned, many Dark Web exchanges continue to thrive and their administrators remain at large.90

Authorities tasked with monitoring the Dark Web face an uphill battle due to the fact that most administrators are constantly changing URL’s multiple times a day.91 And, as one government official has noted, efforts to combat Dark Web commerce are becoming increasingly obsolete as the “assortment of exchanges, virtual currencies and virtual marketplaces have created a complex and evolving environment.”92 Further complicating law enforcement’s effort is the fact that “law enforcement agents are often forced to police in a rapidly evolving age of Internet and digital technology using static, and outdated laws.”93

Moreover, while some in the security community contend that the Dark Web is not completely impenetrable,94 the general consensus is that policing is almost impossible due to “randomness, anonymity . . . and encryption.”95 Policing is further limited because of the simple fact that there are not enough courts, judges, or police officers to tackle the scale of illegal behavior amassed on the Dark Web.96 In response to efforts in the United Kingdom, one leading e-crime expert opined, “the police service is acutely aware of the large and growing problem of cybercrime and is actively working . . . to combat criminality on the web.”97

---

89. Id. (According to the indictment, Ryan Andrew Gustafson created a dark web site “dedicated to manufacturing, selling, buying, distributing and passing of Counterfeit Federal Reserve Notes.”).
90. Andy Greenberg, The Dark Web Drug Lords Who Got Away, WIRED (June 2, 2015), http://www.wired.com/2015/06/dark-web-drug-lords-got-away/. For example, the Marketplace named “evolution” had double the listings as Silkroad and even sold stolen financial information and was operated by the user “Verto” and despite a Homeland security investigation remains at large. Id.
91. See generally Armerding, supra note 71.
92. Remarks of Leslie Caldwell, supra note 45.
94. Armerding, supra note 71.
95. Id.
96. Id.
97. Id.
The most critical issue is the role of anonymous browsing and the risk that it creates. The security community in the United States, specifically the National Security Agency (“NSA”), vehemently opposes anonymous browsing and considers it a threat.\footnote{Abdulmajeed Alhogbani, \textit{Going Dark: Scratching the Surface of Government Surveillance}, 23 \textit{COMM. LAW CONSPectus} 469, 483–484 (2015) (stating “while other branches of the Federal Government are helping fund [Tor’s] service, the NSA has been reportedly waging an ever evolving stealth campaign against the service for years.”).} The NSA claims that Tor and anonymous browsing capabilities should be eliminated because “they are the tools of our adversaries” and are used to coordinate attacks on the United States.\footnote{Id. at 484 (quoting James Clapper, then director of the NSA).} The NSA’s most recent combattting of anonymous browsing was through the EgotisticalGiraffe program.\footnote{Id.} EgotisticalGiraffe allows the NSA to infect users with malware if they download Tor through an outdated web browser.\footnote{Id.} This malware allows the NSA to monitor a downloader’s activity, which is effectively online surveillance.\footnote{Id.} However, those within the cyber security community have called the efficiency of this method into question, labeling it ineffective.\footnote{Id.} This sentiment is due in part to the fact that the monitoring malware only allows the NSA to identify specific users who downloaded Tor on an outdated browser.\footnote{Id. (according to Roger Dingledine, president of the Tor Project, “this method does not allow them to do mass surveillance because ‘[t]here’s no indication they can break the Tor protocol or do traffic analysis on the Tor network.’”).}

IV. SOLUTIONS: SIMPLE ALTERNATIVES AND THE ISSUES WITH CURRENT POLICY

Implementing severe criminal penalties on those convicted of crimes originating on the Dark Web is currently the trend in American jurisprudence.\footnote{See generally Benjamin Weiser, \textit{Ross Ulbricht, Creator of the Silk Road Website Is Sentenced to Life in Prison}, N.Y. TIMES (May 29, 2015), http://www.nytimes.com/2015/05/30/nyregion/ross-ulbricht-createor-of-silk-road-website-is-sentenced-to-life-in-prison.html?_r=0.} However, this should not be the entire focus. Neutralizing the Dark Web threat will require a multi-layered approach, with a focus on both the government and the private sector.

A. General Recommendations

Broadly speaking, there are a few general goals to strive for domestically and internationally in developing strategies to combat the Dark Web threat. The first proposed idea is to map the hidden services directory.\footnote{Chertoff & Simon, \textit{supra} note 29, at 6 (hidden services are all the hidden web sites within the dark web).} This practice allows security agencies to adequately monitor the ever-increasing number of Dark Web
domain names, which is essential because administrators are constantly changing their URL’s.

A related protocol for security agencies and law enforcement would be to analyze web data and “look for connections to non-standard domains.”107 This would result in valuable insight regarding “activities hosted with rogue top-level domains.”108 There are various social sites on the Dark Web that exchange contact information regarding hidden services and strict monitoring of these sites is essential.109

Semantic analysis is another tactic proposed to combat the Dark Web threat. Semantic analysis involves building a cumulative database comprised of all documented hidden services.110 This allows researchers and security agencies to track trends in future illicit enterprises.111 This also allows for marketplace profiling, which is where data is collected about the sellers, users, and transactions being conducted on the Dark Web.112

B. Private Sector Security Measures

Large-scale data breaches typically target private companies and involve personal, financial, and healthcare information.113 The Consumer Privacy Protection Act was introduced in the Senate in 2015 and it imposes certain duties on private companies in the event of a data breach.114 The bill is a response to the fact that, “identity theft is a serious threat to the Nation’s economic stability, national security, homeland security, cyber security, the development of e-commerce, and the privacy rights of Americans.”115 The proposed bill mandates that, “individuals whose personal information has been compromised or who have been victims of identity theft should receive the necessary information and assistance to mitigate any potential damage.”116 Proposed enforcement and penalties include a fine or imprisonment for any individual who “intentionally and willfully conceals the fact of such security breach.”117 The bill authorizes the United States Secret Service and Federal Bureau of Investigation to investigate and enforce the proposed legislation.118

107. Id.
108. Id. (there is a possibility of a privacy issue, yet this could be overcome by only monitoring the destinations and not the specific individual user activity).
109. Id. (for example, Pasterbin—another Dark Web site).
110. Id. at 7.
111. See id.
112. Id.
113. See generally Lanterman, supra note 43; see also Dimarco, supra note 10.
115. Id. at § 2.
116. Id.
117. Id. at § 101.
118. See id. Also, § 103 authorizes federal agencies to unilaterally shut down “BOTNETS” which are a form of malware that allows an attacker to seize control of an individuals’ computer. See id. at § 103.
Moreover, private industries have a duty to develop a “culture of security” in addition to strengthening critical infrastructure.\textsuperscript{119} Some argue that there is another layer of cyber security that goes beyond the digital world, the human element, which is crucial to protecting data from being breached.\textsuperscript{120} This is especially important when networks are accessed via “spear-phishing” attacks.\textsuperscript{121} A spear-phishing attack is when an attacker gathers information about a victim, and then uses that information in an e-mail that contains a malicious link.\textsuperscript{122} The malicious link does not work unless it is clicked on, so a simple preventative measure is companies training their employees to hover above links before clicking to discover the true URL.\textsuperscript{123} A further step is companies ensuring that their vendor contracts contain protective features.\textsuperscript{124} For example, including “audit clauses” would allow an organization to regularly and effectively monitor whether a vendor was complying with necessary standards.\textsuperscript{125} Overall, it is important that the private sector not only strengthen infrastructure, but also employ preventative measures and educate employees.\textsuperscript{126}

V. CONCLUSION

As we move forward in the digital age, there are critical questions that must be answered in order to paint a better picture about the state of cyber security. Does the existence of the Tor network mean that there will always be threats posed by the Dark Web? Is there a more proactive approach to policing the Dark Web than what we have seen so far? Do the benefits of anonymous browsing capabilities outweigh the burden posed by Dark Web cyber criminals? And how far are we willing to go to preserve our privacy online?

Effective policies should aim to cultivate the idea that engaging Dark Web enterprises will result in certain and swift apprehension. The biggest impediment to this concept is the fact that all Dark Web activity retains the ability to remain entirely anonymous.\textsuperscript{127} Moreover, the fact that technology is rapidly advancing keeps Dark Web criminals one-step ahead of law enforcement, who are to struggling to adapt new technology to police the Dark Web.\textsuperscript{128}

The threat posed by the Dark Web is not fully understood. And the emergence of digital crypto-currencies like Bitcoin cast further uncertainty. Nonetheless, a few things should remain in the forefront of future policy makers. Most important is the notion that Dark Web criminals operate more like

\textsuperscript{119} Lanterman, \textit{supra} note 43, at 9.
\textsuperscript{120} \textit{Id.}
\textsuperscript{121} \textit{Id.}
\textsuperscript{122} \textit{Id.} at 8.
\textsuperscript{123} \textit{Id.}
\textsuperscript{124} \textit{Id.}
\textsuperscript{125} \textit{Id.} (simple solutions like this would have prevented the notorious Target hack.).
\textsuperscript{126} \textit{Id.} at 9.
\textsuperscript{127} See generally Chertoff & Simon, \textit{supra} note 34.
\textsuperscript{128} See \textsc{Merchant}, \textit{supra} note 92.
traditional organized crime rings. And as long as the capability to remain anonymous while operating on the Dark Web is still feasible, there will always be a Dark Web marketplace presence, circumventing the law and reaping the profits. If we are to successfully combat this threat there needs to be more collaboration between the federal government and the private enterprises that develop the necessary technology. And until this is realized, every time you go on the Internet you are taking a risk.
AGAINST THE WIND: HAVE WE ACCEPTED DATA BREACH AS AN INEVITABILITY?

Charles Rust

INTRODUCTION

It is no question that data breaches impose a substantial burden upon society.¹ However, the question remains as to who is to bear such a burden. Should the companies storing data be responsible? Should the people relying on companies for data storage suffer the consequences of a breach? Or should the law seek recourse elsewhere, if at all?

Inevitably, opinions regarding data breach liability and privacy standards vary across a broad spectrum.² Some believe the onus should be on the victim, and advocate a risk-reduction strategy which includes common sense elements, such as avoiding suspicious attachments, and employing antivirus software.³ Others have promulgated a national standard requiring the mandatory encryption of personal data.⁴ Yet, others believe companies should be, and in the near future will be, held liable for the negligent storage of information.⁵ Despite these differing views, one reality is clear: big data has become necessary.⁶

An assortment of remedies have been both successfully and unsuccessfully asserted to try and mitigate the damages of data breach, while simultaneously preserving the benefits of data use. Many states now employ notification laws which require breach victims to disclose the occurrence of a breach under appropriate circumstances.⁷ An observable increase in negligence claims

¹. Stephanie Mlot, Cyber Crime Costs the U.S. $140 Billion Annually (Not $1 Trillion), PC MAG (July 23, 2013), http://www pcmag com/article2/0,2817,2422151,00.asp.
resulting from breaches has also occurred. However, most of these actions do not survive summary judgment. Insurance companies have offered their solution to the issue, and the business of “Cyber Insurance” has recently experienced prosperity. Still, the issue of data breaches deserves attention, as the cost of data breaches continues to increase.

Part II of this note will examine the recent history of data breaches over the past ten years, and highlight the more prominent cases during that period. Then, Part III will analyze the current paradigm of legal measures which address breaches. Finally, Part IV of this note will analyze whether the current legal and non-legal remedies offered to victims of data breach are sufficient – and most importantly – whether legal remedies are ultimately necessary.

I. THE GROWING PERVERSIVENESS OF DATA BREACH CASES

Data breach issues have arrived on the forefront of public and private concerns in recent years. The average data breach now costs $3.8 million to remedy, at an average of $154 per stolen or lost record. Some of the most notable cases involving JP Morgan Chase, Target, and Home Depot far exceeded that amount. Organizations victimized by data breach often experience costs related to complying with notification statutes, participating in class-action litigation, and negotiating settlements. Such costs have been illustrated by a plethora of cases, spanning the last decade.

A. TJX: A Prime Example of the Tenuous But Powerful Data Breach Plaintiff

In 2005, TJX Companies was breached by hackers, which spawned six separate actions involving TJX and its banks. The class-action suit against TJX alleged negligence, breach of contract, negligent misrepresentation, and unfair

---

8. Id.
9. Id.
12. Id.
13. Id.
16. A hacker is simply a person who utilizes computers to gain unauthorized access to stored data. Synonymous terms include: cybercriminal, pirate, computer criminal, keylogger, keystroke logger, and more recently, hacktivist.
The district court dismissed the negligence claim under the authority of the economic loss doctrine, which precludes tort damages in the absence of personal injury or property damage. Though the Plaintiffs alleged that the electronic data was property, and therefore had value, the court ruled that the loss was not caused by “the physical destruction of property.” Furthermore, the court refused to limit the economic loss doctrine on policy grounds, thereby avoiding a precedential contradiction.

The court also dismissed the breach of contract claim against TJX, because the Plaintiffs were not a party to the contract. The Plaintiffs alleged that TJX failed to comport with the security standards agreements previously set forth between TJX and lending institutions, and TJX and credit card companies. The Plaintiffs asserted their rights as third-party beneficiaries of those agreements. However, the agreements contained specific language, preventing the conferment of contractual rights and privileges upon third-parties. Thus, the court dismissed the breach of contract claim.

The Plaintiff’s negligent misrepresentation claim against TJX narrowly survived a motion to dismiss. The Plaintiffs asserted that by accepting credit card payments, TJX implicitly represented that it would comply with all security regulations set forth by credit card companies. The court disagreed with the Plaintiffs, characterizing the negligent misrepresentation claim as a negligence claim “without the limitations otherwise applicable to negligence claims.” However, the court found summary judgment to be a more appropriate method of claim disposition in this particular instance, and did not dismiss the claim facially. Lastly, the Plaintiffs contended that TJX’s lack of adequate security measures was an unfair trade practice. Like with the negligent misrepresentation claim, the court deemed it appropriate to await discovery, and utilize summary judgment for disposition of the claim, if appropriate.

Although the preceding claims may seem insubstantial, TJX responded to the threat of prolonged litigation by entering several settlement agreements between

19. Id. at 498 (quoting Aldrich v. ADD Inc., 770 N.E.2d 447 (2002)).
20. Id.
21. Id.
22. Id. at 499.
23. Id.
25. Id.
26. Id.
27. Id.
28. Id. at 494.
29. Id.
30. Amerifirst Bank, 564 F.3d at 495.
31. Id. at 496.
32. Id. at 497.
2007 and 2009. TJX provided customers who could show actual damages with three years of credit monitoring, and paid $6.5 million in attorneys’ fees. The terms of the settlement were estimated to cost TJX $200 million. Subsequently, TJX coordinated with state attorney generals to settle all future claims, which cost them $9.75 million. TJX’s harrowing experience illustrates the potentially dire financial consequences of a data breach to a party defendant.

B. Post-TJX Developments

1. Hannford Bros.

TJX’s case has become a rather common occurrence over the last ten years, with new breaches occurring frequently. In 2007, the Hannaford Bros. grocery chain was breached, allowing hackers access to 4 million credit card numbers. The breach resulted in 1,800 cases of credit card fraud. Hannaford soon became subject to litigation alleging breach of implied contract, breach of implied warranty, breach of duty of a confidential relationship, failure to advise consumers of the theft of their data, strict liability, negligence, and violation of Maine’s Unfair Trade Practices Act. Hannaford is notable, because unlike the court in TJX, the Maine court found the plaintiffs had alleged proper mitigation damages, and held that “plaintiffs need only show that the efforts to mitigate were reasonable, and that those efforts constitute a legal injury, such as actual money lost, rather than time or effort expended.” The court found it entirely foreseeable that a customer who had experienced fraudulent charges would purchase insurance to protect against further consequences of data misuse.

In a later case, this sentiment was not reciprocated by the court when the Plaintiff claimed fear of future harm, but had not experienced fraudulent misuse of her data. Brenda Katz utilized a brokerage firm which, in turn, utilized the Defendant’s brokering account management software. Accountholder tax information and social security numbers were available to users of the software at home, and the Plaintiff claimed this to be an inadequate security measure.

33. See Simon et al., supra note 7.
34. Id.
35. Id.
37. Id.
39. Id. at 162 (quoting In re Hannaford Bros. Co. Customer Date Sec. Breach Litig., 4 A.3d 492, 496 (Me. 2010)).
40. Id. at 165.
41. Katz v. Pershing, L.L.C., 672 F.3d 64, 80 (1st Cir. 2012).
42. Id. at 69.
43. Id. at 70.
2. Heartland Payment Systems

In 2008, the secure data of Heartland Payment Systems was compromised, granting hackers access to the sensitive information of millions of credit card users. The banks which issued these credit cards experienced significant expenses as a result of refunding fraudulent transactions and replacing credit cards, and thus initiated suit against Heartland. The charges against Heartland included breach of contract, negligence, misrepresentation, and violations of multiple state consumer protection laws. All claims against Heartland were dismissed, however, the negligence claim was revived upon appeal. The district court originally dismissed the banks’ negligence claim under the economic loss doctrine, holding that in the absence of physical injury or property loss, recovery would be inappropriate. However, the Fifth Circuit acknowledged that these types of losses are typically limited to contractual remedies.

The court then articulated the policy behind the economic loss doctrine in New Jersey is to reserve claims that the parties could have addressed in their contractual agreement to be resolved by contract law. However, the court noted a precedential exception to the economic loss doctrine in New Jersey, which would allow a foreseeable class of plaintiffs to recover. The court held that, “under New Jersey law, the economic loss doctrine does not bar tort recovery where the defendant causes an identifiable class of plaintiffs to which it owes a duty of care to suffer economic loss that does not result in boundless liability.”

The court ruled the issuer banks were a foreseeable class, because they would suffer harm in the event Heartland Payment was negligent. Payment card information was sent directly from Heartland to the issuer banks, so the identity of the harmed parties, and the nature of the harm were foreseeable.

The court further bolstered its argument by addressing a perceived unfairness to the issuer banks, if they were afforded no remedy in tort law. The court

45. Id.
47. Id. at 422.
48. Id.
49. Id. at 423.
50. Id. at 424 (quoting Spring Motors Distrbs. v. Ford Motor Co., 489 A.2d 660, 671–72 (N.J. 1985)).
51. Id.
52. Lone Star Nat’l Bank, 729 F.3d at 424 (quoting People Express Airlines v. Consolidated Rail Corp., 495 A.2d 107 (N.J. 1985)).
53. Id. at 426.
54. Id.
55. Id.
argued that leaving the issuer banks without a remedy for alleged negligence would “[defy] ‘notions of fairness, common sense and morality.’” It was unclear whether Heartland would be able to take part in dispute-resolution systems regarding fraudulent payments, as the relationships governed by the contracts between Heartland, the Issuer Banks, and the credit card companies were unclear. Furthermore, the Issuer Banks would likely not possess a modicum of bargaining power under any agreements made between Heartland and the credit card companies.

Ultimately, the 2008 breach cost Heartland $140 million. Unfortunately, this was not the end of Heartland’s costly data woes, as they were breached once more in May 2015, when non-encrypted computers were physically stolen from an office building. This was just four months after Heartland announced a warranty, guaranteeing reimbursement for any future breaches. The extent of the breach remains unknown, but Heartland has purchased identity theft protection through an identity monitoring firm.

3. Target

In 2013, Target joined the ranks of data breach victims, when the credit card data of 40 million customers was obtained by hackers. As of January 2015, this particular breach had cost Target $252 million. Target was sued by a class of credit card companies and a class of consumers, alleging violation of consumer protection statutes, violation of data breach statutes, negligence, breach of contract, breach of implied contract, bailment, and unjust enrichment. The Plaintiffs’ unjust enrichment claims survived, on the theory that they “would not have shopped” at Target had they known of the breach, and that “they shopped at Target after Target knew of or should have known of the breach.” While most of the other claims against Target failed, the threat of future lawsuits coerced Target into a $10 million settlement agreement.

56. Id.
57. Id.
58. See Shapiro, supra note 44.
60. Id.
61. Id.
62. Id.
64. Id.
66. Id. at 1178 (emphasis added).
67. See Tabuchi, supra note 63.
4. Home Depot

In November 2014, payment card information of 56 million Home Depot customers was stolen by hackers.68 Home Depot spent $43 million on the breach, in the third quarter of 2014, but expected to recover the amount through its $100 million insurance policy.69 Home Depot was reportedly in compliance with security standards as of 2013, but when the breach occurred, it was undergoing certification for the 2014 calendar year.70 This lapse created the potential for liability, as plaintiffs could allege Home Depot was not in compliance with data breach standards.71

Studies have estimated the potential cost to Home Depot as high as $194 per stolen record, which amounts to over $10 billion by the year 2020.72 Home Depot will likely expend an enormous sum of money investigating the breach, and notifying those parties whose data was compromised. At .49 cents per stamp, notifying all 56 million parties will cost Home Depot $27.44 million.73 They will also need to account for lost business as a result of the breach, and the disruption in business practices caused by the breach. In addition, there are forty four pending lawsuits against Home Depot, which will likely multiply when credit card companies begin suing to recoup their fraud reimbursements to customers.74

5. Sony

Perhaps one of the most memorable breaches was the 2014 breach of Sony Pictures, which caused the delayed release of the film The Interview.75 The hack was allegedly orchestrated by North Korean operatives, because their government did not like the film’s depiction of North Korean Dictator Kim Jong Un.76 This breach arrived on the heels of the April 2011 breach of Sony Online Entertainment.77 In the 2011 breach, the accounts of 102 million users of Playstation Network and Sony Online Entertainment services were

69. Id.
70. Id.
71. Id.
73. Id.
74. Id.
76. Id.
compromised. The affected consumers sued, including the “usual” litany of claims, which Sony exhausted $171 million resolving.

The 2014 breach was much more invasive, exposing not only the data of 6,800 employees and 40,000 business contacts, but also Sony’s future business plans, accounts, and internal structure. Future movies, employee social security numbers, financial plans, and other pertinent documents were also leaked. In March, 2015, eight affected Sony employees filed a class-action lawsuit against Sony, alleging violation of various consumer protection codes, breach of contract, and negligence. Notably, the court found the future monitoring of credit information by the affected employees to be well within reason, and refused to dismiss the negligence claim on those grounds. Not only is Sony coping with the commercial effects of a disastrous data breach, but they are also facing their second major data breach lawsuit in five years.

II. THE STATUS QUO OF DATA BREACH ACTIONS AND REMEDIES

At the time of TJX, the concept of a data breach was relatively novel within the American legal structure. With the occurrence of a multitude of major data breaches in the past 10 years, many courts have had the opportunity to wrestle with the complex issues presented, and some legislatures have also crafted their own responses. Potential data breach litigation is often subject to myriad barriers in the form of damages issues and procedural issues, depending on the nature of the alleged claim. This section will articulate the current state of data breach claims in terms of typical causes of action and the threshold issues each cause of action faces when litigation is commenced.

A. Negligence Actions

Negligence actions are typically alleged as negligent failure to maintain adequate security measures or negligent failure to notify of a breach in a timely manner.

---

78. Id.
80. See Palermo, supra note 77.
81. Id.
82. Id.
84. Id. at *4.
86. DOUGLAS H MEAL & DAVID T. COHEN, PRIVATE DATA SECURITY BREACH LITIGATION IN THE UNITED STATES: INSIDE THE MINDS: PRIVACY AND SURVEILLANCE LEGAL ISSUES LEADING LAWYERS ON NAVIGATING CHANGES IN SECURITY PROGRAM REQUIREMENTS AND HELPING CLIENTS PREVENT BREACHES 3 (Thompson Reuters/Aspatore 2014).
manner. In order to allege negligence, a Plaintiff must establish duty, breach, causation, and damages. While it has been difficult in the past to establish that a Defendant owed a duty to a Plaintiff, courts have generally begun to accept that a Defendant owes a duty if there is a direct relationship between them and the Plaintiff. Duties alleged can range from taking reasonable care to safeguard the secured data of the Plaintiff, to reasonably notifying the Plaintiff of a data breach. Even if a Plaintiff can plausibly allege a duty, the issue of damages still looms in the background.

The damages must flow directly from the breach of duty. Courts have refused allegations of damages due to exposure of data, or destruction of credit cards. In many states, purely economic damages are precluded by the economic loss doctrine. Historically, the economic loss doctrine developed in the products liability context. In the seminal economic loss case, a truck driver sued a brake manufacturer when his brakes failed, damaging his truck. The driver sued for damage and lost profits, but he did not have a contract with the manufacturer. The court barred his action, citing the lack of evidence showing the brake defect caused the injury to his truck.

But some courts, however, have found exception to the economic loss doctrine when the alleged duty is an “independent duty which does not arise from commercial expectations.” An exception also exists when there is an alleged “special relationship” between the parties. Though, these exceptions vary state-by-state, and must relate to the facts of the case.

B. Class Action Issues

A major issue data breach Plaintiffs combat is that of standing. If a data breach Plaintiff cannot establish standing for themselves, they cannot seek relief on behalf of the class. Standing in federal court under Article III can be

---

87. Id. at 6.
89. See id. at 1173.
90. Id. at 1170-71.
91. See MEAL & COHEN, supra note 86, at 44.
92. Id.
94. Id. at 43.
95. See id.
98. See id.
99. See id.
obtained by proving “(1) that [the plaintiff] suffered an ‘injury-in-fact,’ (2) that a causal relationship exists between the injury and the challenged conduct, and (3) that the injury likely will be redressed by a favorable decision.” With regard to injury, a Plaintiff must allege a cognizable injury-in-fact, or that they are in immediate danger of injury due to the alleged conduct. This standard relates to data breach cases, because some plaintiffs cannot allege with certainty that their confidential information was stolen – the only certainty is the possibility that their information was stolen. These types of cases usually result from plaintiffs claiming “increased risk of future harm” as damages occasioning from the defendant’s negligent securitization of confidential information.

Simply put, a split of authority exists Courts are split as to whether a case alleging increased risk of future harm resulting from a data breach confers Article III standing. District courts in Ohio, Washington D.C., Arkansas, and New Jersey have all denied Article III standing on a similar set of facts. Conversely, courts in California, New York, and Connecticut have conferred standing. The courts, which do not confer standing, generally believe that the risk of future harm in such cases is far too speculative.

C. Notification Laws and Related Actions

As a result of the increasing frequency of data breaches, all states except Alabama, New Mexico, and South Dakota have adopted data breach notification statutes. These laws require private or government entities to notify private individuals whose personally identifiable information has been compromised. The laws generally include who must comply with the statute, a definition of “data breach,” requirements for notice, and exemptions. States vary depending on the threshold standard of harm, the form of the data, and who must give notice to render notice effective.

The first state to enact a data breach notification law was California, in 2003. California’s statute requires that all companies doing business in California, regardless of whether they are based in California, give notice to

101. *Id.* at 1050 (quoting Lujan v. Defenders of Wildlife, 504 U.S. 555, 560–61 (1992); Steger v. Franco, Inc., 228 F.3d 889, 892 (8th Cir. 2000)).
102. *Id.* (citing O’Shea v. Littleton, 414 U.S. 488, 494 (1974)).
103. *Id.*
104. *Id.*
105. *Id.*
106. See Amburgy, 671 F. Supp. 2d at 1050-51.
107. See *id.* at 1051.
109. See *id.*
110. See *id.*
112. Cal. Stat. § 1798.82(a) (West 2016).
individuals if their personal data is compromised.\(^\text{113}\) However, California does allow some exceptions. If the compromised information was encrypted, or if the information was publicly available at the time of breach, then the breached organization is not required to provide notification.\(^\text{114}\)

Not surprisingly, there are penalties for noncompliance with the notification statutes. California, for example, affords a private right of action to citizens when a notification statute has been violated.\(^\text{115}\) In other states, like Pennsylvania, the right to sue is retained by the Attorney General,\(^\text{116}\) Notification laws can also differ in their applicability to certain breach occurrences.\(^\text{117}\) These divergences in state law can create difficulties for companies who conduct business in multiple states, as they must comply with a multitude of laws in the event of a breach.\(^\text{118}\)

\section*{D. Insurance Recoveries}

With the risk of loss becoming more apparent, companies are beginning to take measures to mitigate the overall losses caused by a data breach. However, only one in three companies carries insurance which protects against data breach losses.\(^\text{119}\) While appropriate insurance will not fully protect against losses, it can mitigate a sizeable portion of losses and reduce the overall cost of a breach.\(^\text{120}\) So, why would companies choose to forego insurance policies? Some may choose to pass by coverage due to cost, but others may truly believe they are already covered.

Most companies carry what is known as Commercial General Liability insurance (CGL), one of the most common types of insurance coverage.\(^\text{121}\) However, most insurers deny data breach claims under this type of coverage, and contest that CGL policies were never intended to cover data breaches.\(^\text{122}\) Arguments tend to ensue over the specific language of a policy, and whether the loss constitutes a personal injury, property injury, or advertising injury.\(^\text{123}\) This distinction can be as simple as whether a purely electronic record was stolen, or

\begin{itemize}
\item \text{113. See id.}
\item \text{114. See id.}
\item \text{115. Cal. Stat. § 1798.84 (West 2016).}
\item \text{117. See generally id.}
\item \text{119. Michael N. DiCanio, Preparing for the Inevitable: Insurance for Data Breaches, N.Y. L.J. (May 19, 2015), http://www.newyorklawjournal.com/id=1202726774292/Preparing-for-the-Inevitable-Insurance-for-Data-Breaches#ixzz3iERKDOqR.}
\item \text{120. See id.}
\item \text{121. Id.}
\item \text{122. Id.}
\item \text{123. Id.}
\end{itemize}
if the electronic records were contained within a stolen physical medium.\textsuperscript{124} However, insurers are rendering such arguments moot, as they are beginning to include special exclusions in CGL policies, which preclude indemnification for data breach losses.\textsuperscript{125} As a result, companies are exploring alternatives to traditional insurance coverage.

Sometimes, data breach losses can be covered by “crime and fidelity” policies.\textsuperscript{126} These policies generally include coverage for employee dishonesty, money & securities, forgery and computer fraud.\textsuperscript{127} Courts have found that losses resulting from computer fraud, including direct losses and reimbursement losses are included within crime and fidelity coverage.\textsuperscript{128} However, these disputes involve the same types of arguments present in CGL cases between insurers and the insured; such as semantic disputes regarding the meaning of “confidential information.”\textsuperscript{129} This may be why many companies are turning to specialized coverage.

In an effort to avoid disputes caused by ambiguities present in other policies, companies are beginning to carry Cyber Liability Policies.\textsuperscript{130} These policies cover reimbursement of investigation expenses with respect to the cause of a data breach, the cost of engaging a public relations firm, the recovery of electronic data, the losses resulting from business interruption, and the costs of the litigating third-party claims.\textsuperscript{131} However, these policies are new and untested by the courts.\textsuperscript{132} They can include confusing terms, and usually include forum selection clauses, which often aim to place the insured at a disadvantage.\textsuperscript{133} While Cyber Liability Policies are an attractive boon, they should be utilized with caution until they become more established.

III. Analysis

Data breaches are undoubtedly expensive, intricate occurrences, and do not bode well for any organization which experiences them. But how do we, as a society, reconcile the benefits of big data storage with the risks of data breach? Should companies be liable in every facet, expending abhorrent sums of money to reconcile a data breach which may have been unpreventable? Surely,
consumers, employees, and credit card companies have a right to recover their financial losses in the event of a breach. But, is it possible that the prospect of a data breach has become so pervasive, so inexorable, that we must forego the interests of the aforementioned parties to safeguard the survival of society’s businesses and corporations? One Pennsylvania Judge certainly seems to believe so, and I am inclined to agree with him.\textsuperscript{134} It is time for society to cease its penchant for penalizing the very entities which allow it to function as it does. The process of charging corporations with the brunt of data breach consequences may seem like “grabbing the low-hanging fruit,” but in actuality, this tendency may be delaying the advent of a solution to data breach issues.

A proper analysis of data breach resolution demands contemplation of several factors including, but not limited to: (1) The effect upon individuals; (2) The effect upon corporations and business entities; (3) The suitable appropriation of economic consequences; (4) The shortcomings of insurance schemes; and, (5) The virtual inevitability of the harmful criminal activity that characterizes data breaches. The University of Pittsburgh Medical Center [UPMC] was the victim of a data breach, and was subsequently sued by its 62,000 employees and former employees.\textsuperscript{135} Their social security information, names, addresses, bank information, and birthdates were stolen from UPMC’s computer systems.\textsuperscript{136} The Plaintiff class alleged that UPMC did not take reasonable care to safeguard their data, and that UPMC breached a contract with the Plaintiffs.\textsuperscript{137} The Plaintiffs sought the imposition of a duty of care upon UPMC, requiring UPMC to take reasonable care in safeguarding their data.\textsuperscript{138} The Plaintiff’s main obstacle was the economic loss doctrine, which limits purely economic losses to contractual remedies.\textsuperscript{139} Pennsylvania’s narrow exception to the economic loss doctrine allows tort claims when the data is being stored and used for economic gain, however, that was not the case here.\textsuperscript{140} Nonetheless, the court considered five factors used to determine whether a duty should be imposed: “(1) the relationship between the parties; (2) the social utility of the actor’s conduct; (3) the nature of the risk imposed and foreseeability of the harm incurred; (4) the consequences of imposing a duty upon the actor; and (5) the overall public interest in the proposed solution.”\textsuperscript{141} The court considered the consequences of imposing a duty to be too great, and found that doing so would be detrimental to the public interest:

\textsuperscript{135} Id. at *1.
\textsuperscript{136} Id.
\textsuperscript{137} Id. at *3.
\textsuperscript{138} Id. at *5.
\textsuperscript{139} Id. at *2.
\textsuperscript{141} Id. at *3 (quoting Seebold v. Prison Health Servs., Inc., 57 A.3d 1232, 1234 (Pa. 2012)).
Plaintiffs’ proposed solution is the creation of a private negligence cause of action to recover actual damages, including damages for increased risks, upon a showing that the plaintiff’s confidential information was made available to third persons through a data breach. The public interest is not furthered by this proposed solution. Data breaches are widespread. They frequently occur because of sophisticated criminal activity of third persons. There is not a safe harbor for entities storing confidential information.  

This is an interesting proposition. The court went on to consider the effect of data breach litigation on businesses and especially non-profits, and deduced that litigation would likely cause many enterprises to go out of business. In this case, the Defendant was a hospital. It strains credulity that public interest could be served by subjecting a hospital to a multi-million-dollar lawsuit. The Judge correctly recognized that Defendants in data breach cases are also victims, and have their own vested interest in protecting the data of their employees and customers.  

Assuming arguendo that a Plaintiff could successfully assert a negligence claim against a Defendant like UPMC, the cost would be enormous. As stated earlier, the average cost of a data breach in 2015 is approximately $154 per stolen or lost record. Using the data of UPMC’s 62,000 employees, and not counting the former employees whose data was compromised, this data breach could cost UPMC $9,548,000. Something about taking that amount of money from a hospital should feel unconscionable, and that is exactly the sentiment Judge Wettick is expressing.  

There is a growing populace in society who are beginning to accept the inevitability of data breaches. As recently as last year, cyber security expert Dave DeWalt said that “Nearly every company…is vulnerable.” He advocated a more reactive approach to data breaches, explaining that attempts to minimize exposure after a breach occurs are far more effective than working to prevent them outright. According to DeWalt, it takes an average of 228 days to detect a data breach, and even the biggest companies cannot prevent them. Mr. DeWalt’s statistics do not attempt to minimize the negligence of companies who store data, they suggest something entirely different; that it does not matter

142. Id.
143. See id.
144. See generally Dittman, No. GO-14-003285, at *3.
145. See id. at *4.
146. See Rigby, supra note 11.
148. See id.
149. See id.
whether companies are negligently storing data or not, as they will be breached either way.\footnote{150}{See id.}

At this moment, forty-seven states require businesses to notify individuals of a breach, and most include penalties for non-compliance.\footnote{151}{See Davis Wright Tremaine, L.L.P., supra note 111.} Companies must tender this notification at their own expense, which costs \$0.49 per notification.\footnote{152}{The price of a postage stamp.} When breach numbers range from tens of thousands to millions, simply providing notification can be costly. When this is coupled with a devalued reputation, disruption in business, and lawsuits, the costs of a data breach can quickly spiral out of control. Companies should not be subjected to litigation for alleged negligent storage of information.

But what about insurance? One would be incorrect to claim that companies should simply purchase Cyber Liability Insurance. Cyber Insurance is extremely expensive, with premiums varying depending on the insured’s industry.\footnote{153}{Christine Marciano, \textit{How Much Does Cyber/Data Breach Insurance Cost?}, DATA BREACH INS. (June 30, 2015), \url{http://databreachinsurancequote.com/cyber-insurance/cyber-insurance-data-breach-insurance-premiums/}.} According to an insurance provider, a Data Storage Company with a yearly revenue of \$15 million would pay a \$120,000 premium in exchange for \$20 million in coverage.\footnote{154}{Id.} When breaches cost tens to hundreds of millions of dollars, insurance remains a minor factor in mitigating losses of data breach claims.

Data breaches are showing no sign of tapering off in the near future, as more incidences are making themselves apparent. The “cheating site,” ashleymadison.com, was hacked, exposing the records of 37 million customers who utilized the site for their infidelity needs.\footnote{155}{Brian Krebs, \textit{Online Cheating Site Ashley Madison Hacked}, KREBS ON SEC. (July 19, 2015), \url{http://krebsonsecurity.com/category/data-breaches/}.} Not only did the hackers release the personal data of users, but several websites are now offering a service by which users can “plug in” a personal email address and ascertain whether a person used the cheating service.\footnote{156}{Jose Pagliery, \textit{Now You Can Search the Ashley Madison Cheaters List}, CNN MONEY (Aug. 19, 2015), \url{http://money.cnn.com/2015/08/19/technology/ashley-madison-search/index.html?id=EL}.} Though Ashley Madison, advertises one-hundred percent discretion, they also include in the fine-print of the site that they “cannot ensure the privacy or security of the information [users] provide through the internet.”\footnote{157}{Id.} Only time will tell whether this disclaimer will shield Ashley Madison from the pending \$578 million class-action lawsuit.\footnote{158}{See Tanya Basu, \textit{Ashley Madison Faces \$578 Million Class Action Lawsuit}, TIME (Aug. 23, 2015), \url{http://time.com/4007374/ashley-madison-578-million-lawsuit-canada/}.}
Likewise, a class action lawsuit was filed against Experian on July 17, 2013, after it was discovered that a hack exposed 200 million consumer records.\textsuperscript{159} The facilitator of the breach then sold the stolen data to criminals, who then used the information to commit identity theft.\textsuperscript{160} It is estimated that over 13,000 people have been victimized thus far, by the filing of $65 million in fraudulent tax returns.\textsuperscript{161} The lawsuit against Experian seeks to impose a notification requirement on Experian, provide credit monitoring services to affected parties, disgorge all profits of the breach, and establish a reimbursement fund to remediate the financial effects of identity theft.\textsuperscript{162}

Experian and AshleyMadison are not the only victims either. As of August 4, 2015, a total of 466 breaches had occurred, allowing access to 139,265,185 records.\textsuperscript{163} 35.8\% of those breaches occurred in the medical and healthcare industries.\textsuperscript{164} United Airlines, the world’s second largest airline has reported a potential hack, which could potentially expose customer information as well as United’s internal business strategies.\textsuperscript{165} However, since the customer data is composed of names, birthdates, and addresses, it is not likely that United will be statutorily required to notify affected parties.\textsuperscript{166} What is likely though, is that there will be another data breach, sooner than later.

Because breaches are growing more prevalent, American institutions are beginning to accept them as everyday life. One would speculate this does not bode well for American consumers. However, American consumers are consistently the most unaffected parties in data breach scenarios. An overwhelming majority of the time, the only real harm experienced by consumers is a speculative risk of future harm.\textsuperscript{167} An individual victimized by data breaches experiences no diminution in the value of their personal identifying information.\textsuperscript{168}

Furthermore, entities are beginning to take steps to insulate individuals from harm. Every credit card issuer in the country exempts cardholders from paying

\begin{itemize}
\item \textsuperscript{159} Brian Krebs, \textit{Experian Hit With Class Action Over ID Theft Service}, \textsc{Krebs On Sec.}, (July 21, 2015), http://krebsonsecurity.com/2015/07/experian-hit-with-class-action-over-id-theft-service/#more-31682.
\item \textsuperscript{160} \textit{See id.}
\item \textsuperscript{161} \textit{Id.}
\item \textsuperscript{162} \textit{Id.}
\item \textsuperscript{164} \textit{Id.}
\item \textsuperscript{166} \textit{Id.}
\end{itemize}
fraudulent charges. Yet, consumers are treated as if they have no protection at all. It seems apparent that virtually everyone is aware of data breaches, or else they would not be developing countermeasures. Perhaps an appropriate query is whether consumers should be subject to a “pseudo-assumption of the risk,” since the nature of data breaches is so blatantly obvious.

Assuming the aforementioned is a valid question, can we in good conscience place even a portion data breach culpability on the American public? Probably not. People are not going to boycott companies who store data, because it has become too necessary. Businesses and corporations will likely continue to bear the brunt of data breach costs, because they are the easiest target and public perception seems to indicate they are the most apt to absorb the burden. But are they really the most responsible? Entities which store data can only follow the regulations that are in place, and are limited by the bodies which impose those very regulations, aka the legislature.

There is growing sentiment calling for legislators to clearly define the data breach landscape with national data security standards. Proponents assert that financial institutions and credit unions are subject to federal regulation under legislation like the Gramm-Leach-Bliley Act, and opine that other entities who handle sensitive personal data should be subject to similar treatment. They advocate flexible standards, which are scalable from the smallest business to the largest. It is possible that uniform standards will help alleviate the current data security predicament. However, this scenario remains predominantly speculative until actual legislation occurs.

IV. CONCLUSION

Data breaches have become commonplace in today’s society. While the solution for the past ten years has been to allow breached organizations to bear the brunt of data breach losses, this cannot continue indefinitely. Not every company that is breached can bear the financial burden of complying with notification statutes, addressing internal issues related to the breach, providing fraud insurance to affected parties, paying possible fines, and fighting class action lawsuits. Many of these cases end in million dollar settlements, which have the potential to cripple businesses for years to come. Courts should follow the example of the Court of Common Pleas of Allegheny County Pennsylvania, and dismiss data breach claims against entities.

Data breaches are simply a cost of doing business, for both companies and consumers. Though it is difficult for plaintiffs to commence actions against

171. Id.
172. Id.
companies following a data breach, often the threat of a lawsuit can lead to a costly settlement. This seems a bit counterintuitive, when the most well-protected data can be breached just the same as lesser-protected data. At what point have consumers assumed the risk of utilizing data storage, or doing business with an organization which utilizes data storage? After all, data breaches are quickly becoming a staple of modern society. There must be a way to hold negligent organizations responsible without subjecting them to limitless liability.¹⁷³ Some legislatures have attempted to do so with Notification Laws and consumer protection laws, but any cohesive action is lacking. For now, it does not matter whether a person is a plaintiff or a defendant in a data breach case, they are a victim, and they are fighting a virtually unwinnable war.

The recent hacks into Sony, Ashley Madison, and other large companies have directed consumers’ attention to the fact that their data may not be as secure as they previously expected. As it turns out, many of the world’s largest companies are not even employing minimal data security measures to protect sensitive personal information, like credit card and social security numbers, which has not gone unnoticed by the Federal Trade Commission. The F.T.C. has been taking action against companies for having these unfair data security practices.

While various companies have challenged the F.T.C.’s authority to take these actions, the United States District Court for the District of New Jersey decided—and was later affirmed by the Third Circuit—in *F.T.C. v. Wyndham Worldwide Corp.* that the F.T.C. Act did give the agency the authority to regulate practices in this area. This article posits that the holding of *F.T.C. v. Wyndham*, as well as other existing data security law, support the argument that the F.T.C. Act authorizes the F.T.C. to regulate unfair data security practices. It will also discuss the inefficiencies of other methods of data security regulation and why it is imperative that the F.T.C. continue to have enforcement authority in this area.

I. INTRODUCTION

In November 2014, the sky fell on the entertainment industry. One of its biggest companies, Sony, was hacked, revealing employee information like social security numbers, employee emails, movie scripts, and executives’ salaries. The public was given a rare look at the internal politics of Sony, seeing who the favorite and least favorite actors to work with were, how much diversity existed among top executives, and other similar pieces of information. A few of Sony’s highly anticipated new films, like “The Interview” and “Annie,” were
even made available online. This came as quite a shock to Sony employees, who believed that their emails, records, and other projects were private and secure.

Over the last few years, high-profile hacks have haunted consumers and companies alike. Hackers caused Target to re-issue over one hundred million credit cards, and also stole credit card numbers from over fifty million Home Depot customers. Most recently, hackers were able to access the records of thirty-seven million users of AshleyMadison.com, a controversial service that aims to help individuals have extramarital affairs. These hackers, who call themselves the “Impact Team,” released the information of all thirty-seven million users, including email addresses and credit card information. While this hack may seem to some as the users receiving their just deserts, it illuminates the fact that companies’ methods of storing personal information are not nearly as secure as some might expect them to be.

This is not surprising considering the current status of cybersecurity law. While there are some federal statutes governing the security measures that entities must take with respect to sensitive personal data, these statutes only apply to specific industries and do little to encourage companies outside of the covered industries to impose more stringent security procedures. There are also state statutes in this area; however, they vary widely and focus more on notice after a hack than on preventing hacks from occurring.

This lack of consensus and uniformity across all industries has created a situation where there are not many incentives for companies to take advanced measures to ensure the security of their data. Consumers generally only suffer minimal damages and negligence claims against hacked companies are rarely successful. If these lawsuits continue to fail and fines are not imposed, companies will take little action to ensure that the sensitive, personal information

2. Id.
3. Id.
5. Id.
9. E.g., KY. REV. STAT. ANN. § 61.933 (West 2015) (requiring companies in Kentucky to notify customers of a breach of their personal information within thirty-five days after the conclusion of an investigation into the breach).
of their employees and consumers is protected. Yet, incentives could be put into place.

The Federal Trade Commission (F.T.C.) is currently trying to increase security by bringing administrative actions against companies for having unfair data privacy practices. In the past, it took action against companies for misrepresenting their data security policies. Now, the F.T.C. is taking data security a step further by enforcing the idea that companies who store sensitive personal data must take reasonable security measures to prevent information breaches. In addition to providing an incentive for companies to employ more secure practices, this could also help raise awareness that the Internet is not an inherently safe place, as many business leaders lack an understanding of data security risks. However, some of its targeted companies have challenged the F.T.C.’s authority to regulate the field of data security.

This article argues that the F.T.C. should have the authority to regulate unfair data privacy practices. Part II reviews relevant federal and state data security statutes. Part III discusses the Federal Trade Commission Act and how the F.T.C. has used the authority this Act purportedly grants. Part IV provides a summary of *F.T.C. v. Wyndham Worldwide Corp.*, the first case to address the question of whether the F.T.C. has authority to regulate unfair data privacy practices. Finally, part V discusses alternative solutions, but ultimately demonstrates why it is both appropriate and important that the F.T.C. regulate data privacy practices, consistent with *F.T.C. v. Wyndham*.

II. BACKGROUND LAW

Currently, there are various federal and state statutes that revolve around data security. The federal statutes tend to impose data security standards only for specific industries. On the other hand, state statutes typically focus on the steps that need to be taken after a data breach occurs. The F.T.C. has even tried to use its authority in this area by bringing claims against entities that use unfair or

11. *See Susskind, supra note 4, at 594.*
15. *E.g., LabMD, Inc. v. F.T.C., 776 F.3d 1275 (11th Cir. 2015).*
17. *E.g., OHIO REV. CODE ANN. § 1349.19 (West 2015) (focusing on acceptable methods of notification).*
deceptive data privacy practices.\textsuperscript{18} The following sections discuss the framework of these federal and state data security statutes, as well as the statutory authority of the F.T.C..

A. Federal Statutes

There are various federal statutes in existence that attempt to regulate data privacy practices in different industries. However, Congress has yet to publish a blanket statute that imposes security requirements across all industries handling personal information of consumers. In general, these currently enacted statutes require companies within the covered industries to disclose their privacy practices and exercise care in handling consumer data.\textsuperscript{19} Some even mandate that companies implement specific safeguards to prevent data breaches.\textsuperscript{20} The most well-known of these statutes are the Gramm-Leach-Bliley Act and the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

The Gramm-Leach-Bliley Act primarily regulates financial institutions;\textsuperscript{21} however, there have been attempts to expand the reach of the Act to cover other businesses.\textsuperscript{22} The Act requires financial institutions to take measures to ensure the security and confidentiality of their customers’ nonpublic information and other records and to inform customers of their data privacy policies.\textsuperscript{23} The Act has given many agencies the authority to promulgate and enforce data security regulations, including the F.T.C. and others affiliated with the Department of the Treasury.\textsuperscript{24}

Similarly, HIPAA regulates the data security practices of businesses that handle personal health information. It requires healthcare entities to provide notice of their privacy practices to customers\textsuperscript{25} and implement the security measures the Department of Health and Human Services promulgates to protect personal information that is collected from customers.\textsuperscript{26} However, enforcement of this statute has been weak.\textsuperscript{27}

Other federal agencies, like the Department of Defense, require contractors to take certain data security measures in order to do business with the government.\textsuperscript{28} Specifically, the Department of Defense requires contractors to

\begin{itemize}
  \item \textsuperscript{18} Scott, supra note 13, at 129.
  \item \textsuperscript{21} 15 U.S.C. § 6801 (2012).
  \item \textsuperscript{22} Andrea M. Matwyshyn, \textit{Data Devolution: Corporate Security, Consumers, and the Future of Regulation}, 84 Chi.-Kent L. Rev. 713, 718 (2010).
  \item \textsuperscript{23} 15 U.S.C. §§ 6801, 6803 (2012).
  \item \textsuperscript{25} Matwyshyn, supra note 22, at 716–17.
  \item \textsuperscript{26} 42 U.S.C. § 1320d-2 (2012).
  \item \textsuperscript{27} Matwyshyn, supra note 22, at 717.
  \item \textsuperscript{28} Thaw, supra note 24, at 297–98.
\end{itemize}
implement the information systems security program specified by the National Institute of Standards and Technology. If these controls are not put into place, the contractor must provide a written explanation of why the controls are not applicable or what alternative controls it will use as equivalents. However, all of these federal data security requirements only apply to specific companies. They do not cover all industries that maintain collections of sensitive consumer data.

As for attempts to prevent the improper dissemination of information thought to be private from the other end of the spectrum, there is a federal statute that criminalizes hacking called the Computer Fraud and Abuse Act (CFAA). Specifically, this statute makes it a crime to intentionally access a computer without authorization and obtain financial information, information from a protected computer, or other valuable pieces of information. A protected computer is defined as any computer that affects or is used in interstate or foreign commerce. Thus, this statute protects businesses that store sensitive personal information on computers. Yet, this statute does nothing to encourage or require companies to take measures to prevent hacks into the systems on their end.

The industry-specific statutes have helped advance the data protection goals within the covered industries, but they do not cover businesses throughout the entire economy that handle sensitive consumer data. Therefore, a blanket federal statute covering all entities storing sensitive information would be necessary, absent F.T.C. regulatory action, to incentivize the protection of this data.

B. State Statutes

States have also attempted to deal with data security threats in the increasingly cyber world. Forty-six states, the District of Columbia, and a few U.S. territories have enacted laws requiring institutions that have suffered a data breach to notify individuals whose information has been compromised. These laws generally revolve around when notification of a breach is necessary, rather than what protective measures are required to prevent a breach. However, the

30. Id.
32. Id.
33. See id.
35. Thaw, supra note 24, at 297.
wording and requirements of these statutes differ from state to state, meaning there is no uniform method for notification.37

For example, following the discovery that a California resident’s data was breached, persons or entities that conduct business in California must notify the resident whose unencrypted information was accessed.38 There is no set time frame for making these disclosures; they must only be made in the “most expedient time possible.”39 Methods of notification are relatively standard across all state statutes, but the requirements for substitute notice (email, posting on the business’s website, or notification to statewide media) differ across states.40 In California, before entities are permitted to provide substitute notice, they must demonstrate that the cost of providing notice exceeds $250,000, or the affected class exceeds 500,000 people.41

The Kentucky statute, on the other hand, is quite different from its California equivalent. Kentucky only requires “agencies,” which are defined as different branches and subsections of the government, including public schools and government-created entities,42 to implement security measures.43 Other entities within Kentucky that store personal information must notify the individuals affected only after notifying various commissioners and secretaries within the state and conducting an investigation.44 These commissioners and secretaries must be notified within seventy-two hours after determination of a security breach and affected individuals must be notified within thirty-five days of the conclusion of the investigation.45 Unlike California, Kentucky does not have threshold requirements for when posting notice of the breach on the entity’s website or notification of media outlets is acceptable.46

39. Id.
40. Compare, e.g., Cal. Civ. Code § 1798.82(j)(3) (West 2016) (requiring an individual to provide substitute notice consisting of email, website posting, or notification on statewide media if the cost of statutory notice is excessive, the size of the affected class is excessive, or sufficient contact information is unavailable), with Ky. Rev. Stat. Ann. § 61.933(2)(a)3 (West 2015) (requiring notice to individuals of the type that is most likely to result in actual notification), and Ohio Rev. Code Ann. § 1349.19(E)(4)-(5) (West 2015) (requiring an individual to provide substitute notice consisting of email, website posting, or notification on statewide media if the cost of statutory notice is excessive or sufficient contact information is unavailable, and distinguishing the requirement for substitute notice for a business entity with ten or fewer employees to include notification by paid advertisement), and Ariz. Rev. Stat. Ann. § 44-7501.D.4 (2016) (requiring substitute notice consisting of email, website posting, or notification on statewide media if the cost of statutory notice is excessive or sufficient contact information is unavailable).
43. Id. § 61.932. “Security measures” are not defined in the statute, nor are they expressly required to be reasonable under a plain reading of the statute.
44. Id. § 61.933(1)(a).
45. Id. § 61.933(1)(b)(1).
46. See id. § 61.933.
Ohio does not have any statutory requirements for its businesses or agencies to take reasonable security measures; it focuses solely on notification after a breach and what types of notice are acceptable.\(^47\) In Ohio, any person that owns or licenses computerized personal information must disclose any breach of the data to residents of the state whose information was accessed, if the access reasonably might cause a material risk of identity theft or fraud.\(^48\) These disclosures must be made in the most expedient time possible within forty-five days after discovery of the breach.\(^49\) Ohio has the same requirements as California as to the use of substitute notice methods.\(^50\)

As is clear through these few examples, there are many differences among state data security statutes. The biggest differences are usually in the time frames for disclosures. Some statutes, like Kentucky’s, have multiple time frames for different affected individuals and government officials; others have no set time frame at all, such as California and Arizona.\(^51\) There are even differences in the types of data breaches that must be disclosed. For example, California and Ohio only require the disclosure of a breach into unencrypted information, while Kentucky requires it for personal information in general.\(^52\) Thus, companies that do business across the country may find it difficult to comply with all of the various state data breach statutes.

### III. The Federal Trade Commission Act

Given the gaps and inconsistencies in data security law, the F.T.C. has recently begun bringing enforcement actions against companies that have not been using appropriate data security practices.\(^53\) If the F.T.C. is able to continue regulating this area, it will fill the gaps in federal law and bring consistency to data security requirements across the country.\(^54\) However, some companies and commentators have argued that the F.T.C. lacks the authority to regulate.\(^55\)

The Federal Trade Commission Act established the F.T.C. in 1913 and gave the commission the authority to take action against any “person, partnership, or corporation [that] has been or is using any unfair method of competition or unfair or deceptive act or practice in or affecting commerce…”\(^56\) The F.T.C. may

---

48. Id. § 1349.19(B)(1).
49. Id. § 1349.19(B)(2).
53. See Bailin, supra note 12.
54. See generally Cave, supra note 10, at 780.
55. See Scott, supra note 13, at 159 (discussing that the application of the unfairness doctrine to data security breaches may be an unwarranted use of the doctrine).
declare that any practice is unfair if it is likely to cause substantial consumer injury that is not reasonably avoidable or outweighed by benefits to consumers, or if it is contrary to established public policy.\textsuperscript{57} Thus, actionable unfair practices are not confined by statute to certain categories of business practices, like advertising, but can be any practice that affects commerce and causes substantial injuries to consumers.\textsuperscript{58}

The F.T.C. has used its authority to penalize companies for using many different types of unfair and deceptive practices.\textsuperscript{59} For example, in the past, the F.T.C. has successfully brought claims against companies who were using false or misleading advertisements.\textsuperscript{60} It has also used its authority to prevent companies from selling products at unreasonably low prices to shut out competition.\textsuperscript{61} In addition to these enforcement actions, the F.T.C. regularly issues guidelines on best business practices, which help companies create policies that are in harmony with the F.T.C.’s ideas of fairness.\textsuperscript{62}

Recently, as individuals have begun living more and more of their lives online, the F.T.C. has started using its authority to take action against companies that use unfair data security practices.\textsuperscript{63} Since 2002, the F.T.C. has filed complaints against over forty companies that have engaged in these practices, and almost all cases resulted in settlements requiring the companies to increase their data security.\textsuperscript{64} In these settlements, the F.T.C. typically required companies to implement data security programs with “administrative, technical, and physical safeguards” that were appropriate based on the company’s size and complexity.\textsuperscript{65} The settlements also generally required companies to perform risk assessments in order to address vulnerabilities in their computer systems and to continually monitor the effectiveness of their security procedures.\textsuperscript{66}

\textsuperscript{57} Id.
\textsuperscript{58} See generally id. (defining unfair as an act or practice causing substantial injury to consumers without enumerating specific business acts that would produce this injury).
\textsuperscript{60} See, e.g., News Release, Fed. Trade Comm’n, FTC Sends Refund Checks Totaling Nearly $6 Million to Consumers Who Bought Dietary Supplements (Dec. 20, 2013), 2013 WL 6698681 (detailing actions against Central Coast Nutraceuticals for deceptively advertising an acai berry supplement as a weight-loss product and a colon cleansing supplement as an aid for preventing cancer).
\textsuperscript{61} See, e.g., In re Standard Brands Inc., 46 F.T.C. 1485 (1950).
\textsuperscript{62} See, e.g., FED. TRADE COMM’N, PROTECTING PERSONAL INFORMATION: A GUIDE FOR BUSINESS 3 (Nov. 2011), https://www.ftc.gov/system/files/documents/plain-language/bus69-protecting-personal-information-guide-business_0.pdf. This F.T.C. resource allows companies to see how their practices measure up to the best practices and see where changes are necessary.
\textsuperscript{63} Id., supra note 12.
\textsuperscript{64} Id.
\textsuperscript{65} Id.
\textsuperscript{66} Id.
Only a few companies thus far have challenged the ability of the F.T.C. to regulate data privacy practices and impose these types of requirements. One of these companies was an Atlanta-based laboratory called LabMD. The F.T.C. began investigating LabMD’s data privacy practices after the company suffered a data breach of sensitive patient information. The F.T.C. then filed an administrative complaint alleging that LabMD had been engaging in an unfair practice “by failing to prevent unauthorized access to its patient information.” LabMD sought an injunction to stay the action, claiming that the F.T.C. had no authority to regulate protected health information. However, the District Court for the District of Columbia refused to hear LabMD’s claims because the administrative proceeding was not yet final. Thus, this challenge did not shed any light on the F.T.C.’s authority to regulate data privacy practices.

Although data privacy is vital to consumers, there remains a lack of congressional guidance on the future of the F.T.C.’s authority to regulate data privacy practices. Congress also has yet to pass a comprehensive statute incentivizing companies across all industries to protect sensitive information. F.T.C. v. Wyndham, however, provides guidance to other courts in deciding whether the F.T.C. has authority to regulate in this area. And, frankly, Wyndham represents the appropriate move forward in cybersecurity law with respect to personal data.

IV. F.T.C. v. Wyndham Worldwide Corp.

Wyndham Worldwide is a hospitality business that franchises and manages hotel chains and timeshares. Wyndham hotels are independently operated, but they must use a Wyndham Worldwide computer system that manages reservations and credit card payments for all of the hotels in the chain. These computer systems store customers’ personal information, such as addresses and credit card numbers, and are all linked to the corporate Wyndham network.

68. See LabMD, 776 F.3d at 1277.
69. Id.
70. Id.
71. Id. at 1277–78.
72. Id. at 1280.
73. See id.
74. See Cave, supra note 10, at 780.
75. Id.
76. See infra Part IV.
78. Id. at 608.
79. Id.
reservations for Wyndham-branded hotels go through the same corporate website.\textsuperscript{80}

Between 2008 and 2011, this corporate network was hacked on three separate occasions.\textsuperscript{81} The hackers used similar methods to access the system on all occasions.\textsuperscript{82} Yet, according to the F.T.C., Wyndham failed to take steps to prevent the third breach even after discovering the first two.\textsuperscript{83} More than 619,000 payment card numbers were stolen through these breaches, leading to over $10.6 million in fraud loss.\textsuperscript{84}

As a result of these breaches and investigations into Wyndham’s conduct, the F.T.C. sought an injunction against Wyndham to prevent it from engaging in more activities that unreasonably expose customers’ personal information to unauthorized individuals.\textsuperscript{85} The F.T.C. brought this action under the authority of Section 5 of the F.T.C. Act, which allows the F.T.C. to take action against those who use unfair or deceptive practices that affect commerce.\textsuperscript{86} In response, Wyndham filed a motion to dismiss, primarily arguing that the F.T.C. lacked the authority to bring an unfairness claim in relation to data security.\textsuperscript{87} Wyndham also argued that the F.T.C. should have promulgated regulations before asserting an unfairness claim, and that it failed to plead all elements of an unfairness claim.\textsuperscript{88}

After analyzing Wyndham’s argument that the F.T.C. lacked authority in the data security sphere, the United States District Court for the District of New Jersey decided that the F.T.C. did have authority to regulate unfair data security practices.\textsuperscript{89} Wyndham argued that, because there were federal statutes regulating data security in small sectors of the economy, the F.T.C. was precluded from creating general data security standards for the whole private sector economy.\textsuperscript{90} But the court failed to see how the F.T.C. asserting unfairness authority over data security practices would be incompatible with recent legislation or contradict congressional policy.\textsuperscript{91} The court viewed the federal statutes as complimentary to the F.T.C.’s authority, giving the F.T.C. extra tools to enforce reasonable data security measures.\textsuperscript{92} When affirming the district court’s decision, the Third Circuit even suggested that the recent privacy legislation would have been

\begin{itemize}
\item \textsuperscript{80} Id.
\item \textsuperscript{81} Id.
\item \textsuperscript{82} Id.
\item \textsuperscript{83} F.T.C. v. Wyndham Worldwide Corp., 10 F. Supp. 3d 602, 608 (D.N.J. 2014), aff’d, 799 F.3d 236 (3d Cir. 2015).
\item \textsuperscript{84} Id. at 609.
\item \textsuperscript{85} Id. at 608.
\item \textsuperscript{86} Id. at 607.
\item \textsuperscript{87} Id.
\item \textsuperscript{88} Id.
\item \textsuperscript{89} See Wyndham Worldwide, 10 F. Supp. 3d 602 at 610.
\item \textsuperscript{90} Id. at 611.
\item \textsuperscript{91} Id. at 612.
\item \textsuperscript{92} Id. at 613.
\end{itemize}
inexplicable without the F.T.C.’s already existing authority in this area. Thus, both courts agreed that the F.T.C. could use its “unfairness authority” in data security issues.

Both courts were also unconvinced by Wyndham’s arguments that the F.T.C. failed to provide fair notice by promulgating formal regulations. Wyndham attempted to argue that, because it had not published any guiding regulations, the F.T.C. had violated “bedrock principles of administrative law.” However, the district court found that common law does not require the F.T.C. to publish regulations before taking action under its unfairness authority. Instead, the decision of whether or not to publish regulations was left to the discretion of the F.T.C.

Even if notice were required, the district court discussed how promulgating regulations was not the only way for the F.T.C. to provide notice of what constitutes an unfair practice. Indeed, Section 5 of the F.T.C. Act contains a three-part test for what practices are unfair, the F.T.C. has made public statements about data security, and the F.T.C. has even released a guidance brochure on the topic.

The Third Circuit had an even stronger response to Wyndham’s fair notice argument, deciding that Wyndham was only entitled to a very low level of notice, which was satisfied by the statutory definition of unfair practices. This definition clearly informed Wyndham that its data security practices would be subject to a cost-benefit analysis and by failing to encrypt any customer data, restrict any IP addresses, or require any password changes, Wyndham should have known that its conduct would fail the analysis. Therefore, Wyndham’s second argument for dismissal failed to convince either court.

Wyndham’s last argument was that the F.T.C. had failed to adequately plead its unfairness claim, specifically by failing to plead a substantial injury to consumers that the consumers could not reasonably avoid. Federal law places a $50 limit on consumer liability for unauthorized charges on a credit card and credit card companies can rescind these charges. Thus, Wyndham argued that

---

94. See id.
96. Id. at 616.
97. Id. at 619.
98. Id.
99. See id. at 620.
100. Id. at 619–20.
102. Id. at 255–56.
104. Id. at 622.
105. Id. at 621.
the harm to consumers could not be substantial.\textsuperscript{106} Yet again, this argument was unsuccessful.\textsuperscript{107} The circuit court did not directly address this argument. But according to the district court, an injury could be substantial if it caused a small amount of harm to a large group of people, or if it created a significant risk of harm.\textsuperscript{108} The court cited the 619,000 compromised credit card numbers and $10.6 million in fraud loss to show that the F.T.C. had adequately pled this kind of substantial injury.\textsuperscript{109} Also, the court decided that Wyndham’s failure to use readily available security measures, like firewalls, was enough at this stage to lead to a conclusion that the company had caused the substantial injury.\textsuperscript{110} Therefore, the court denied Wyndham’s motion to dismiss.\textsuperscript{111}

The District Court of New Jersey and the Third Circuit were two of the first courts in the country to issue opinions on the relatively new issue of whether or not the F.T.C. has the authority to regulate data privacy practices.\textsuperscript{112} The district court even shed some light on how the substantial injury requirement can be met. Given the increasing importance of data privacy, other courts should look to these opinions in dealing with future challenges to the F.T.C.’s authority in order to continue promoting the security of sensitive consumer data.

V. ANALYSIS

A. The F.T.C.’s Authority to Regulate Data Security Practices as Unfair Practices

A popular argument that those opposed to the FTC’s authority to regulate data security practices have made is that the mere fact that a company has suffered a breach cannot be an unfair practice.\textsuperscript{113} However, this argument fails to take into account the bigger picture.\textsuperscript{114} Breaches may draw the F.T.C.’s attention to certain companies, but they are not unfair practices on their own.\textsuperscript{115} The unfair practice in these cases is the companies’ failure to implement and maintain adequate security measures, unreasonably putting sensitive consumer information at risk.\textsuperscript{116} Companies that store sensitive information are aware of the devastating

\textsuperscript{106} Id. at 622.
\textsuperscript{107} See id.
\textsuperscript{108} Id. at 623.
\textsuperscript{109} Wyndham Worldwide, 10 F. Supp. 3d at 622.
\textsuperscript{110} Id. at 624.
\textsuperscript{111} Id. at 631.
\textsuperscript{113} Scott, supra note 13, at 143.
\textsuperscript{114} See id.
\textsuperscript{115} See generally Fed. Trade Comm’n, supra note 62 (discussing enforcement actions against companies for failing to implement certain security measures).
\textsuperscript{116} See Wyndham Worldwide, 10 F. Supp. 3d at 624 (discussing how Wyndham failed to implement complex password or adequately inventory computers on the Wyndham network, which constituted the “unfair practice”).
effects its unauthorized release can have. Yet, some still fail to keep security in line with the nature of the information.117

Luckily, the F.T.C. has the authority to take action against entities that engage in unfair practices that affect commerce.118 An unfair act or practice is generally defined as an act or practice that “causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.”119 Therefore, for an act or practice to be unfair, there must be: (1) an actual or likely substantial consumer injury, (2) which is not reasonably avoidable, or (3) outweighed by a consumer benefit.120 The F.T.C. can also consider public policy along with other evidence of unfairness.121

As discussed previously, the act or practice in this context is failing to take reasonable security measures to protect sensitive data. Reasonable security measures do not have to be overly complex or expensive.122 They could involve simply updating firewalls, encrypting data, and assessing security systems on a routine basis.123 These practices are minimal considering the gravity of the information that is stored in company computers. As they are so minimal, a cost reduction or consumer benefit argument cannot justify failure to put measures into place.124 Yet, many companies have not been performing these basic tasks, resulting in many of the hacks that have recently given news outlets fodder for discussion.125

Such omissions played a large role in the hacks that were involved in *F.T.C. v. Wyndham*. According to the court, Wyndham failed to implement simple measures to protect its consumer data, like requiring passwords to be complex.126 This is an extremely simple measure that Wyndham could have taken.127 Wyndham also neglected to properly inventory the computers that were connected to its system to ensure that only authorized computers were accessing

---

117. See generally Susskind, *supra* note 4, at 583 (discussing the sensitive categories of personal information that hackers have successfully stolen off of company databases).


120. See id.

121. Id.

122. See Susskind, *supra* note 4, at 584, 587 (discussing a case where hackers were able to steal all client records of CorporateCarOnline because the company had not updated its firewall in eight years and had failed to encrypt its data, which are some of the most basic and obvious data security measures a company can take, and also listing simple steps that companies can employ to heighten security).

123. See id.

124. See id. at 586 (stating that a free security update could have prevented a data breach in 2008 as an example of simple, minimal security measures that many people fail to take).

125. Id. at 585.


it, or use firewalls to limit unauthorized access. The F.T.C. alleged that these measures clearly constituted an unreasonable failure to take simple data security measures given that customer addresses, credit card numbers, and other sensitive information were stored within Wyndham’s network.

Breaches occurring as a result of a company’s failure to take these actions can satisfy the second prong of the unfairness definition. A breach of personal data is a substantial injury for many reasons; the first of which is monetary. Experts have estimated that an average breach costs a total of $5.4 million, costing consumers an average of $157 per record exposed. While these losses are small on an individual scale, as a whole they represent a substantial loss of funds that could have been used much more productively. As the court in F.T.C. v. Wyndham correctly concluded, Wyndham customers suffered a substantial loss, as their fraud loss totaled $10.6 million, almost doubling the average.

The consumers themselves could not have reasonably avoided these losses. The court in Wyndham did not address this point because it was too fact-dependent, but given that consumers now live in an almost entirely cyber world, this prong of the unfairness doctrine is clearly met. When consumers trust companies with their personal information, they have an expectation, however misguided, that their information will be protected. These expectations arise quite frequently, as it is estimated that online transactions total $3.7 trillion annually in the United States, and $10 trillion globally. In fact, online transactions represented about twenty-one percent of GDP in the United States. Quite simply, individuals and companies are conducting a significant amount of transactions online. Given this commercial environment, consumers

---

128. Wyndham Worldwide, 10 F. Supp. 3d at 624.
129. Id. at 608.
130. Id. at 625.
131. See Peters, supra note 36, at 1173 (discussing the cost of data breaches on consumers collectively).
132. See id.
133. See Susskind, supra note 4, at 600 (implying that passing on the costs of a breach to consumers hurts the economy as a whole).
134. Wyndham Worldwide, 10 F. Supp. 3d at 609.
137. See Commercial Data Privacy in the Internet Economy, supra note 137, at 14.
138. See id. at 18.
139. Id. at 14.
cannot be expected to avoid having their personal information stored in company networks.\textsuperscript{141}

It is often argued that consumers should pay attention to privacy policies and avoid the use of technologies that do not promise high levels of security.\textsuperscript{142} If they did, consumers would be able to have a sense of security about their data.\textsuperscript{143} However, this argument is extremely unrealistic. Consumers do not have the time to read all of the fine print in privacy policies.\textsuperscript{144} Generally, when consumers see that a company has a privacy policy, they believe that it sets limits on the company’s ability to share their information.\textsuperscript{145} This leads consumers to expect that the company will exercise care in protecting consumer information from unauthorized persons.\textsuperscript{146}

Although companies may not make such promises, these expectations are entirely reasonable on the part of consumers.\textsuperscript{147} They are trusting companies with the keys to their lives.\textsuperscript{148} Companies know this and should take appropriate action. Although Wyndham customers most likely expected that they would be safe making reservations with such a large and respected chain, Wyndham left them vulnerable by not taking appropriate data security measures.\textsuperscript{149}

Allowing a breach to occur by failing to take reasonable security measures also causes serious, intangible damage to consumers and to the economy as a whole.\textsuperscript{150} When consumer data is stolen, consumers suffer an extreme violation of privacy.\textsuperscript{151} Suddenly, a stranger knows where they live, what their email addresses are, and even what their social security numbers are.\textsuperscript{152} Even if this does not result in much financial damage, the consumers still are left feeling violated and insecure.\textsuperscript{153} Allowing this to continue to happen by not penalizing unfair security practices does not comport with American notions of the importance of privacy.\textsuperscript{154} Personal information needs to be protected; its protection is crucial to maintaining the well-being and freedom of American

\begin{itemize}
\item 141. See \textit{COMMERCIAL DATA PRIVACY IN THE INTERNET ECONOMY}, supra note 137, at 14.
\item 142. See \textit{Scott}, supra note 13, at 161.
\item 143. Id.
\item 144. See \textit{Cave}, supra note 10, at 766.
\item 145. \textit{COMMERCIAL DATA PRIVACY IN THE INTERNET ECONOMY}, supra note 137, at 18.
\item 146. Id.
\item 147. Id.
\item 148. See \textit{Susskind}, supra note 4, at 576–77, 583. Addresses, email addresses, bank account information, and credit card information are examples of some of the sensitive information company databases maintain.
\item 150. See \textit{COMMERCIAL DATA PRIVACY IN THE INTERNET ECONOMY}, supra note 137, at 13.
\item 151. See id. at 10 (noting that when hackers gain access to private consumer information, the consumers right to control their personal information is seriously impaired).
\item 152. See \textit{Susskind}, supra note 4, at 576, 583, 592 n.102.
\item 153. See \textit{Seal}, supra note 1 (admitting that Sony employees were “coming to work afraid” after their personal information was released by hackers).
\item 154. See \textit{COMMERCIAL DATA PRIVACY IN THE INTERNET ECONOMY}, supra note 137, at 9.
\end{itemize}
society.\textsuperscript{155} Yet, there are still some who argue that because breaches of personal data only impose a small monetary cost, there is no real harm done to consumers.\textsuperscript{156}

The loss of consumer trust that comes with a data breach is another harm to both consumers and the economy.\textsuperscript{157} Consumer trust is fundamental to online commerce.\textsuperscript{158} If major data breaches continue to occur at the rate that they have been over the past few years, trust in the Internet marketplace is going to continue to spiral downwards.\textsuperscript{159} The decreased consumer trust will likely manifest itself in a loss of competitiveness in the global economy, as consumers inside and outside of the U.S. will steer their business away from insecure American companies.\textsuperscript{160} While the court in Wyndham did not focus on these types of harms, courts should consider them in deciding whether an act or practice is unfair in future data security cases for policy reasons.\textsuperscript{161}

Although it is unlikely that Wyndham or any other company that has suffered a data breach wanted hackers to access their customers’ information, the failure of these companies to put into place reasonable security measures undoubtedly made it easy for hackers to access the information.\textsuperscript{162} This is clearly unfair under the language of the F.T.C. Act, given the substantial injuries consumers suffer.\textsuperscript{163} Therefore, regulating this unfair practice falls within the umbrella of the F.T.C.’s authority.

\textbf{B. The F.T.C.’s Authority and Other Federal Law}

Even if unfair data security practices fall within the scope of the F.T.C.’s authority, some feel that federal statutes, like the Gramm-Leach-Bliley Act and HIPAA, preempt its authority.\textsuperscript{164} A review of these statutes, however, shows that they do not contradict the F.T.C.’s authority. As discussed previously, these Acts require financial and healthcare institutions, among others, to take certain measures to protect their customers’ personal information, and give enforcement authority to certain regulatory agencies.\textsuperscript{165} For example, the Gramm-Leach-Bliley Act gives authority to a number of agencies other than the F.T.C. to regulate data

\textsuperscript{155} Id.
\textsuperscript{156} See Scott, supra note 13, at 157.
\textsuperscript{157} See Fed. Trade Comm’n, supra note 62, at 2.
\textsuperscript{158} Commercial Data Privacy in the Internet Economy, supra note 137, at 15.
\textsuperscript{159} Id.
\textsuperscript{160} See id. at 6 (discussing the importance of the US developing a data privacy framework that allows consumers both within and outside the US to have trust in United States companies in order to encourage innovation and allow multinational companies to operate smoothly).
\textsuperscript{161} See generally id. at 13 (discussing that addressing intangible harms is vital to the United State’s continued global competitiveness).
\textsuperscript{162} Susskind, supra note 4, at 583–85.
\textsuperscript{163} See id. at 576–77 (describing the various losses from hacks that were easily preventable).
security, including the Bureau of Consumer Financial Protection, state insurance authorities, and other regulatory bodies. The Act gives each agency authority over a specific section of the financial sector.

The Gramm-Leach-Bliley Act gives the F.T.C. authority over “any other financial institution or other person that is not subject to the jurisdiction of any agency or authority under [previous subsections].” Rather than confining the F.T.C. to regulating data security in these specific institutions, this section of the Gramm-Leach-Bliley Act serves more as a confirmation that the F.T.C.’s authority to regulate data security practices in the financial sector was not taken away. The Act did nothing to take away the F.T.C.’s authority to regulate unfair practices in this area in general.

Federal data security laws serve to protect sectors where data security is of the utmost importance by giving regulatory agencies like the F.T.C. extra enforcement tools. As the court in Wyndham correctly noted, these extra protections are entirely complimentary to the F.T.C.’s pre-existing authority. This is especially true considering Congress intended “unfair acts and practices” to be a flexible concept that was not tied to a particular statutory or common-law standard. The flexibility of this concept has been extremely important in allowing the F.T.C. to adapt its actions to the ever-evolving economy, and is even more vital now due to the rapid pace of technological change.

Therefore, due to the intentionally flexible nature of the F.T.C.’s authority to regulate unfair practices and the complimentary nature of federal data security laws, the Wyndham court was correct in deciding that the F.T.C. retained authority to take action against unfair data security practices. The security of personal information is important across all industries, not just in some. The fact that personal information is given protection in some industries should not mean that such protection is precluded in others, especially when there is a federal body authorized to give that protection.

167. See id. (giving the Board of the National Credit Union Administration authority over any federally insured credit union, and the Security and Exchange Commission authority over investment companies, brokers, and investment advisers).
168. Id.
169. See Wyndham Worldwide, 10 F. Supp. 3d at 613.
171. Wyndham Worldwide, 10 F. Supp. 3d at 613.
172. Id. at 615.
175. See id. at 612–17; see also Am. Fin. Servs. Ass’n, 767 F.2d at 967–68.
176. See generally COMMERCIAL DATA PRIVACY IN THE INTERNET ECONOMY, supra note 137, at 9 (discussing that protecting the privacy of consumers is critical to the value of the Internet as a whole).
C. Fair Notice

Another legal issue that companies have raised with respect to the F.T.C.’s authority over unfair data security practices is whether the F.T.C. must first promulgate official regulations before it can take action against companies.\textsuperscript{177} Wyndham argued that the F.T.C. had provided no guidance whatsoever regarding the appropriate data security measures, and the Commission therefore could not hold them liable.\textsuperscript{178} As discussed previously, the court decided that the F.T.C. was not required to promulgate regulations to provide notice before taking action.\textsuperscript{179} However, even if fair notice were required, the F.T.C. has released multiple documents that would fulfill the requirement.\textsuperscript{180}

For example, in 2011, the F.T.C. released a business guide detailing principles that would help businesses keep their data secure.\textsuperscript{181} These principles include: keeping track of all computers and other devices where sensitive information is stored; only storing what is needed for business to be conducted; encrypting sensitive information; and running updated spyware programs.\textsuperscript{182} The guide went into detail about all of the different measures that companies should take in order to keep sensitive consumer and employer information safe.\textsuperscript{183} Although the guide was not overly technical, it was enough to spread some awareness that certain measures needed to be taken.\textsuperscript{184}

Settlement agreements between other companies that have practiced unfair data security practices and the F.T.C. have been released for the public to review.\textsuperscript{185} In these settlements, the F.T.C. required unfair practices to be discontinued and required companies to perform ongoing security assessments.\textsuperscript{186} The F.T.C. has also mandated that infringing businesses adopt rules requiring strong passwords that need to be changed periodically, implement firewalls to control access, and train employees on security policy.\textsuperscript{187} A review of the specific requirements of the settlements ought to be enough to give a business a good idea about what a proper data security plan looks like.\textsuperscript{188}

If the business guides and settlements are not considered enough, the definition of “unfair acts or practices” in the F.T.C. Act provides companies with

\begin{itemize}
  \item \textsuperscript{177} See Wyndham Worldwide, 10 F. Supp. 3d at 616–17.
  \item \textsuperscript{178} Id.
  \item \textsuperscript{179} Id. at 617–21.
  \item \textsuperscript{180} See, e.g., \textit{FED. TRADE COMM’N}, supra note 62.
  \item \textsuperscript{181} See generally id.
  \item \textsuperscript{182} Id. at 5–11.
  \item \textsuperscript{183} Id. at 5–11.
  \item \textsuperscript{184} Id. at 2.
  \item \textsuperscript{185} See generally Bailin, supra note 12.
  \item \textsuperscript{186} Thaw, supra note 24, at 337.
  \item \textsuperscript{187} Bailin, supra note 12 (describing the settlement requirements as falling into seven categories: privacy, security, software/product review, service providers, risk assessment, unauthorized access/disclosure, and employee training).
  \item \textsuperscript{188} See id.
\end{itemize}
an idea of what will be expected of them. The definition is intentionally flexible; it allows the F.T.C. to address situations that Congress could not possibly enumerate in a piece of legislation. Although its flexibility does not give businesses concrete practices to follow, the definition still provides a helpful framework to develop the best data security practices. At the very least, it alerts businesses to the fact that action may be taken against them if their practices are causing substantial injury, no matter what those practices might be.

Taken together, the F.T.C.’s business guides, settlement agreements, and the definition of “unfair practices” provide businesses ample notice that they must take reasonable data security measures or face the threat of F.T.C. enforcement. Clearly, formal regulations are not the only way to provide notice of what is expected of companies. Thus, the court correctly rejected Wyndham’s argument that the F.T.C. should have been disallowed from proceeding in the data security field without promulgating regulations.

D. The Importance of the F.T.C. ’s Authority

It is very important that other courts follow the lead of the District of New Jersey and the Third Circuit. This is true not only because their decisions were in accordance with the F.T.C. Act and other federal statutes, but also because the F.T.C. is in the best position to increase the security of consumer and employee data.

The F.T.C. is better suited to regulate data security practices than states for two major reasons. The first of which is that the states do not focus on the most important issues. State data security laws tend to focus on notice and disclosure of data breaches, rather than on preventing them from occurring. These statutes do too little too late. Notification is important to curb damages, but by the time the notification of a breach has been made, consumers have already suffered a substantial amount of harm. However, F.T.C. enforcement actions are beginning to fill the absence of data breach prevention in state law.

Even if states were to pass data breach prevention statutes, they still would not be better suited than the F.T.C. to regulate in this area because the statutes

190. See id. at 616–18.
191. See generally id.
192. See generally Fed. Trade Comm’n, supra note 62; see also generally Bailin, supra note 12.
194. Id.
195. See Susskind, supra note 4, at 575; see also Peters, supra note 36, at 1173. Peters indicates that, even with data breach notification laws, fraud loss still totals $5.4 million per incident, while Susskind discusses how these losses are passed on to consumers.
196. See Bailin, supra note 12.
would likely vary in the same ways that data notification statutes do.\textsuperscript{197} This is the second reason why the F.T.C. is better suited than states to regulate in this area: state statutes vary too widely to give adequate protection.\textsuperscript{198} When confronted with various state notification statutes, the inconsistencies leave businesses confused and unsure as to how they should proceed.\textsuperscript{199} This is a frequent occurrence, likely due to the interstate nature of modern commerce.\textsuperscript{200} The companies with the most personal data to protect are the ones with customers from multiple states, or even multiple countries.\textsuperscript{201}

For example, Target and Home Depot, two companies that were recently hacked have customers from across the nation.\textsuperscript{202} Ashley Madison, another recently hacked company, has 37 million users, who could live just about anywhere, as it offers web-based dating services.\textsuperscript{203} In theory, these companies should have researched multiple state notification statutes to ensure that they were in compliance with all of them.\textsuperscript{204} In reality, these companies likely chose one or two methods and time frames and hoped they would comply with all the state laws.\textsuperscript{205} This is not how companies should be addressing data security. But, if left to the states, data security practices could continue down this unreliable path. The F.T.C.’s authority is important to resolve the inconsistencies in state law and focus the trajectory of data security practices across the national marketplace.\textsuperscript{206}

Federal laws are similarly insufficient to address consumer data security. Currently, federal law only narrowly requires specific industries or industries with specific clientele to take appropriate data security measures.\textsuperscript{207} While the data in those industries is undoubtedly sensitive, there are many uncovered companies that harbor similar personal information.\textsuperscript{208} The mere fact that a customer’s social security number is stored in a non-financial or non-medical institution’s computer system does not render it undeserving of some level of secure treatment. That is why the F.T.C.’s authority in this area is so important—it fills the gaps and is perfectly complementary to federal data security law.

If the F.T.C.’s authority were taken away, many of the incentives that currently exist for companies to take reasonable data security measures would

\begin{enumerate}
\item \textsuperscript{197} \textit{See} Peters, supra note 36, at 1198.
\item \textsuperscript{198} \textit{See} id. at 1185.
\item \textsuperscript{199} \textit{See} supra note 10, at 782.
\item \textsuperscript{200} \textit{Id.} at 787–88.
\item \textsuperscript{201} \textit{See} id.
\item \textsuperscript{202} \textit{Susskind, supra} note 4, at 576.
\item \textsuperscript{203} \textit{Pagliery, supra} note 6.
\item \textsuperscript{204} \textit{See Cave, supra} note 10, at 788–89.
\item \textsuperscript{205} \textit{See} id.
\item \textsuperscript{206} \textit{See generally} Peters, supra note 36, at 1181, 1184 (discussing the necessity of a broad and consistent approach to data security regulation).
\item \textsuperscript{207} \textit{See} 15 U.S.C. §§ 6501–05 (2012) (protecting the online data of children under 13).
\item \textsuperscript{208} \textit{See generally} Peters, supra note 36, at 1171 (describing the sensitive account information that hackers were able to obtain from retail stores, like Target and Home Depot).
\end{enumerate}
disappear. As discussed previously, the average breach costs about $5.4 million. The value of money tends to be greater to an individual than to a large company, thus the company might take less care than an individual would to ensure the security of information. Also, as the threat of hacking is illusive, occurring in the non-visual cyberworld, companies tend not to see data breaches as serious risks. Even after companies are hacked and have to deal with the consequences, they do not seem to feel the need to increase security. Wyndham was hacked three times before the F.T.C. stepped in and filed a complaint, with Wyndham all the while using out-of-date firewalls and other weak security practices. Thus, the threat of a hack alone is not enough to incentivize companies to implement reasonable security measures.

The F.T.C., however, has the ability to increase incentives if it retains authority. Through increased enforcement, the F.T.C. can make companies aware that they will face legal action if they are not using reasonable data security practices. This could be the case even if they have not suffered a data breach. Being the subject of an enforcement action means that a company will have to pay legal fees, costs associated with settlement compliance (including training employees and possibly developing a new data security department), and perhaps even penalties. The threat of these extra costs, combined with the threat of breach notification costs, will be strong incentives for a company to comply with reasonable data security principles.

Aside from being able to provide incentives, the F.T.C. is also in a unique position that will allow it to have the best response to consumers’ data security needs. Security in the cyber-world is a continuously evolving concept. When secure programs are created, hackers find vulnerabilities in them and manufacturers update the programs to get rid of the known weaknesses. New ways to access and protect data are discovered regularly. Because of the rapidly changing and increasingly vulnerable nature of the cyberworld, companies and governments alike have taken to hiring the world’s best hackers

---

209. See Thaw, supra note 24, at 341.
211. See Susskind, supra note 4, at 600 (discussing the ability of businesses to pass costs on to consumers).
212. Id. at 593.
214. Id.
215. See Susskind, supra note 4, at 593–94.
216. 15 U.S.C. § 45 (2012). The injury requirement under this statute can be fulfilled if the practice is likely to cause substantial consumer injury, actual injury does not have to occur.
218. Thaw, supra note 24, at 341.
219. See Susskind, supra note 4, at 586.
220. Id. at 575.
to point out flaws in their computer systems and develop top of the line security programs.221

Given this data security climate, it would be difficult to pin down a single standard that would adequately protect a company’s sensitive consumer information.222 But the F.T.C. does not have to. As discussed previously, the F.T.C.’s authority is over a flexible class of practices.223 It is able to use its discretion in deciding what is unfair and what is not, and it is able to adapt its decisions to advances in technology, changes in the market, and other developments.224 In this way, the F.T.C. is not tied to any one method of enforcement, meaning it does not have to wait for lengthy amendment processes to be completed in order to change its enforcement tactics. This unique position makes the F.T.C. the best candidate to regulate data security practices.

However, there are still some actions that the F.T.C. must take to effectively regulate data security. While formal regulations are not necessary, it is advisable that the F.T.C. regularly issue guidelines to increase awareness about simple but necessary security measures.225 Currently, there is a lot of misunderstanding in the corporate world about hacking threats and data security practices.226 Regular business guides could help clear up some of this confusion and encourage companies to develop new security programs geared toward cyber threats.227 Being educated on the topic will do a lot to make company leaders understand the importance of protecting their customers’ data.228 It also will ensure that companies know they will be held accountable for lax security. Additionally, it is important that guides reinforce the idea that companies need to be flexible with their data security practices and routinely monitor and update them.229

Another recommendation is for Congress to pass comprehensive federal legislation that reinforces the F.T.C.’s authority to regulate data security and establishes uniformity in current data security law.230 This could be something as simple as mandating companies that handle sensitive data to implement and maintain reasonable data security measures, without going into specific measures.231 The F.T.C. already has the authority to mandate this, but such a

222. Scott, supra note 13, at 140.
224. See id.
225. See Susskind, supra note 4, at 585–86 (discussing that most companies have a very limited awareness of cybersecurity threats).
226. See id.
227. See Cave, supra note 10, at 788.
228. See id. at 788.
229. See Peters, supra note 36, at 1198.
230. See Scott, supra note 13, at 171.
231. See id. at 171–73.
statute could end the debate and remove uncertainty about the F.T.C.’s authority. Federal legislation could also impose breach notification standards to resolve the discrepancies in state statutes and allow companies to comply more easily.

VI. CONCLUSION

The F.T.C.’s authority is extremely important in regulating data security practices. If it were taken away, a void would be left that state or federal action would not likely fill. In time, companies may face pressure from competition and other market conditions to increase security on their own, but this will not happen quickly enough to adequately protect the information of vulnerable consumers and employees across the United States. The F.T.C. is an immediate solution to the data security problem, and has already helped to increase the protection of this information. If the F.T.C. were to continue down its path of data security regulation, consumers would likely face less data threats and develop more confidence in the cyber marketplace. This would be a big step forward for cyber privacy and the economy in general.

Without F.T.C. guidance, data breaches like the ones Sony, Ashley Madison, Target, and Home Depot suffered would become much more common. This would impact more of the economy than just the cyber-market, as more and more funds would have to be used to clean up attacks rather than to develop new products or services. Also, privacy, which has always been such an important American value, would become all but nonexistent. No one wants to live in a world where the notion that privacy does not exist is the norm.

232. See id. at 141.
234. See Susskind, supra note 4, at 594.
235. See COMMERCIAL DATA PRIVACY IN THE INTERNET ECONOMY, supra note 137, at 13–14.