COLUMBIA UNIVERSITY
JOURNAL OF POLITICS & SOCIETY

Web Feature: Wednesday, February 18, 2015
Editor: Chris Meyer, Executive Editor (2013-2014)
Author: Haley Lepp, Georgetown University

Where Innovation and Citizen Safety Intersect: The Future of American Big Data Regulations

Haley Lepp
Science, Technology, and International Affairs
School of Foreign Service
Georgetown University
May 5, 2014

Abstract: The rise of information technology has created an unprecedented amount of data and data-producing technologies. The collection, storage, and use of consumer data grow at an increasing rate as more devices connect to Internet of Things. As data analysis becomes a necessity for competition in all industries and for the success and efficiency of government workings, the potential for misuse of consumer information intensifies. New technologies and industry standards leave consumers unaware of data collection. A lack of standards for secure collection and storage of data leaves room for vulnerabilities. The aggregation of information from various sources can present dangerously intrusive pictures of an individual. To avoid these misuses, Congress must supplement the current consumer protection framework regulated by the Federal Trade Commission with a Consumer Bill of Rights. This bill, originally introduced by the Obama Administration, must be developed by all stakeholders and should focus on outcomes instead of specific technology practices.

Data, the Game Changer

The rise of information technology and technologized objects has led to such an explosion of information that it has become commonplace to refer to our time as the Information Age. IBM boasts that the world creates 2.5 quintillion bytes of data every day. The same report estimates that 90 percent of all information in the world has been created in the last two years alone.[i] Popularly referred to as Big Data, the enormous datasets produced by modern technology can be caught, stored, aggregated, and analyzed to provide an invaluable and increasingly necessary tool for all participants in the global economy[ii]. The Economist Intelligence Unit, in a 2012 survey, found that nine out of ten business leaders would describe data as a fourth factor of production comparable to land, labor, and capital.[iii]

Until recently, collected data sets consisted solely of "actively published" information, i.e."names, addresses, telephone numbers, email addresses, gender, age, marital status…profession, income level."[iv] Even if consumers did not intend to publicize information, they were aware that such data existed. In recent years, however, the information explosion that has accompanied the increase of information technology in consumer culture has given rise to new technologies that collect and publish data without consumer knowledge. These technologies, ranging from smartphones to digital watermarks, collect, connect, and communicate data on such an unprecedented level that they are changing the very makeup of the Internet.

Sometime between 2008 and 2009, the number of "things" connected to the Internet surpassed the number of people connected. Scientists and Internet leaders refer to this phenomenon as the Internet of Things (IoT). [v] A Cisco report claims that there were 12.5 billion devices connected to the Internet in 2010, almost twice the world population at the time of 6.8 billion. This is an even bigger feat considering that only a fraction of the world population is

connected to the Internet. The same report estimates that by 2015, there will be 25 billion devices connected through the Internet, a number expected to double by 2050. Though sources vary greatly in numerical predictions -Gartner expects 30 billion- all predict that connected devices will increase exponentially in the coming years.[vi]

The IoT encompasses more than just phone or tablet-like devices. The term describes a revolutionary development in Internet function, namely, the communication between mundane objects. Any "thing," from a refrigerator to a thermostat to a car, that can communicate with another "thing" can and will contribute to these ever-expanding networks.[vii] Scientists and entrepreneurs around the world are devising innovative ways to connect physical objects to create and use data. Wireless sensors in the ears of cattle, implanted by a Dutch start-up company, help agriculturalists to monitor animal health.[viii] Phones, cars, and other objects equipped with geolocation systems produce spatial coordinates and time stamps of user movements.[ix] Nest Labs, recently acquired by Google, has developed a thermostat application that collects data from other devices to determine the weather, power prices, and even the movements of specific individual inhabitants with different temperature preferences.[x] As a result of these connected objects, the nature of the data being produced has changed. Instead of census-style, human-produced information, we can now collect massive amounts of passively produced information, from geographical points to temperature, pressure, vibration, and stress.[xi]

Data, the Commodity

Data-producing, connected products are no longer an industry of their own. Connectivity is quickly becoming a necessity for modern competition. A *Harvard Business Review* article postulates that established producers in traditional industrial fields "have to protect the turf they

already own… while pursuing growth through service offerings that leverage the fact that the product is in place to offer a richer overall value proposition to customers."[xii] Traditional product companies are left with the choice of connecting to the IoT or being left behind. As more industries connect their products to the IoT, data collection will also grow.

The value of these devices, according to Thomas Lee, a Stanford University electrical engineering professor quoted in the *Wall Street Journal*, is "secondary to the services they enable." The use of consumer data to "tailor outreach to individual consumer computers or mobile devices," a trend coined by the advertising and marketing industries, is now relevant and applicable in almost all fields.[xiii] As of 2010, Oracle, IBM, Microsoft, and SAP together spent over $15 billion on data management and analytics firms, a business growing almost twice as fast as the entire software industry and estimated to be worth over $100 billion.[xiv] Gartner Inc. expects worldwide sales in the data industry to reach over $300 billion by 2020, a number dwarfed by the expected total economic savings from improved productivity: $1.9 trillion.[xv]

Much of the value of this industry depends on the collection, storage, and analysis of consumer data. For example, the ability to track consumers in order to offer more personalized online advertisements, "effectively subsidize[s]" an entire industry of free software and applications.[xvi] Profits from the online advertising industry allow developers to create innovative new products for a wide range of audiences. Consumer tracking and other forms of big data analytics also have the potential to "enhance how the government administers public services," create systems more respectful of civil rights, and encourage accountability across the public sector. Yet even John Podesta, Counselor to the President, warns, "big data tools also unquestionably increase the potential of government power to accrue unchecked."[xvii] Podesta cites government use of census data during World War II to track and detain Japanese Americans

in internment camps as a historical example of potential misuses of citizen information. The private sector, too, demonstrates the potential to endanger consumers through marketing discrimination, increased tracking, and insecure collection and storage methods. Even if private sector industries limit collection, current rules allow the government to obtain data from the private sector or outsource to the private sector analytics projects that are not legal in the public sector.[xviii]

The Intersection of Privacy and Innovation

To ensure that big data analytics can help both private and public sectors to realize their full potential while also protecting citizen rights, legislation across all sectors must be developed to prevent misuse of data. In February of 2012, the Obama Administration proposed a Consumer Bill of Rights. Though this proposition, ironically, did not succeed on Capitol Hill because of the concurrent scandal surrounding Edward Snowden and the NSA surveillance leaks, President Obama has continued to push for more consumer/citizen protection. In January of 2014, in his remark on Review of Signals Intelligence, the president called for Podesta and the Council of Advisors on Science and Technology (PCAST) to lead "a comprehensive review" of the issues surrounding big data and privacy.[xix] This review culminated on May 1, 2014, with the release of two parallel reports: *Big Data: Seizing Opportunities, Preserving Values*, and *Big Data and Privacy: a Technological Perspective*. The reports suggest that current legislation must be updated and developed to ensure consumer security, continued innovative practices, and international interoperability. Both reports, along with recent publications by other legislative entities, argue that a key facet of developing sustainable and effective legislation is the

identification and accommodation of the definition of privacy, a definition that continues to evolve as society grows more connected through social technologies.

PCAST, in this report, argues that the term "privacy" includes retaining secrecy in personal matters, the ability to selectively share information, the ability to make "intimate personal decisions without government interference," and protection from discrimination based on characteristics such as race or gender.[xx] Three main themes emerge from the privacy concerns outlined in these documents and publications by the Federal Trade Commission, various pieces of state and federal legislation, and international reports of data privacy: use of consumer data in unexpected ways, insufficient protection of collected consumer data, and overly intrusive analysis due to dataset aggregation.

Edith Ramirez, Chairwoman of the Federal Trade Commission, claimed in the Commission's 2013 Internet of Things Workshop that one of the main privacy challenges posed by big data is the collection and use of information in ways that consumers do not expect.[xxi] This challenge manifests in consumer knowledge of initial data collection and in the ownership and potential aggregation of collected information. A 2011 study by Cornell University Electrical and Computer Engineering professors Stephen Wicker and Robert Thomas demonstrates that signals from WiFi networks can reveal the number of people in a room and each person's location within the room.[xxii] The ability of the Internet provider or a third party to collect this information, or the use of such information for commercial or government purposes, may not be revealed to customers at the time of purchase. Even if companies do alert users of data collection practices, a Senate Report on the data broker industry published in December of 2013 claims that "it is unclear whether… [consumers] understand the extent to which data concerning their offline activities also may be collected".[xxiii]

Consumers may also be unclear about who collects or has access to their information. Data brokers, defined by the Federal Trade Commission as "companies that collect information, including personal information about consumers… for the purpose of reselling such information to their customers for various purposes, including verifying an individual's identity, differentiating records, marketing products, and preventing financial fraud" are a common third party owner of consumer information.[xxiv] Because such companies rarely come in direct contact with consumers, most consumers are unaware that data brokers may be collecting their data.[xxv] One of the largest of such companies, Acxiom, caters to customers that include, according to a 2013 United States Senate report,

> 47 Fortune 100 clients; 12 of the top 15 credit card issuers; seven of the top 10 retail banks; eight of the top 10 telecom/media companies; seven of the top 10 retailers; 11 of the top 14 automotive manufacturers; six of the top 10 brokerage firms; three of the top 10 pharmaceutical manufacturers; five of the top 10 life/health insurance providers; nine of the top 10 property and casualty insurers; eight of the top 10 lodging companies; two of the top three gaming companies; three of the top five domestic airlines; six of the top 10 U.S. hotels.[xxvi]

While Acxiom's wide range of prominent clients demonstrate the growing necessity to leverage the power of Big Data in order to compete, they also demonstrate the growing frequency with which the average consumer comes in contact with the data industry. In fact, many of the most prominent data brokers have contracts with companies that limit company disclosure about data sources.[xxvii] Even when approached by the Committee on Commerce, Science, and Transportation for research on the 2013 Senate Report, the three largest broker industries

(Acxiom, Experian, and Epsilon), were "secretive," refusing to identify either the sources of their data or their specific customers.[xxviii]

A second major risk to privacy, as identified by President Obama in his 2012 proposal, Chairwoman Ramirez in the Federal Trade Commission Workshop, and other publications, is the lack of standards for data protection in all parts of the data industry. For example, consumer data can be intercepted as it is collected, a problem given recent media attention due to the discovery of the Heartbleed Bug. The bug derives from a vulnerability in OpenSSL, an open-source software used to establish secure connections between web browsers and servers.[xxix] Though OpenSSL is maintained by a small group of volunteers, nearly 66 percent of websites are built around SSL and thus compromise consumer information.[xxx] Until overarching inter-industry standards are established to dictate secure collection techniques, consumer data will remain vulnerable to attack.

Even if data is collected in a secure way, preserving anonymity is becoming increasingly challenging. The NIST *Guide to Protecting the Confidentiality of Personally Identifiable Information* (SP 800-122) defines personally identifiable information (PII) as

> any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information[xxxi]

As more abstract data become available due to more devices connected through the IoT, these distinguishing characteristics become more ambiguous. Geospatial metadata, for example, can potentially provide a connection to personally identifiable information in the physical world,

though it is not included in this definition. Aggregation of collected statistics can also provide a comprehensive picture of a consumer, despite the harmlessness of such pieces of data individually.

To protect PII, companies and government organizations use a variety of methods to de-identify data, including anonymization, pseudonymization, encryption, key-coding, data sharing. However, as hackers and scientists alike develop ways to re-identify anonymized data, these standard methods have been repeatedly shown to only temporarily de-identify PII.[xxxii] Podesta, in his May 2014 report to the president, warns that significantly more effort and investment goes into re-identification methods than research to obscure personally identifiable information and enhance privacy. Storage methods, too, pose threats to consumer information. Epsilon, one of the most prominent American data brokers, suffered a breach in 2011 which exposed the names and email addresses of thousands of consumers, clients of Capital One, JPMorgan Chase, Citibank, and many other companies.[xxxiii] Axciom had a similar breach in 2003.[xxxiv] Until standards for collection and storage of consumer data are legislated, we will, as the FTC's 2012 report warns, "pay a price if data…through a security breach falls into the wrong hands."[xxxv]

The third, and arguably most powerful challenge to privacy is what analysts refer to as the Aggregation Effect. Data brokers and other collectors that retreive information from government records and other public data, purchase or license information from other data collectors, access other databases from agreements with other companies, or mine self-reported information directly from consumers, have the ability to form a much more comprehensive picture of an individual. Julie Cohen, the Georgetown University Law professor who coined the term "Aggregation Effect," notes "[a] comprehensive collection of data about an individual is vastly more than the sum of its parts."[xxxvi] The Supreme Court has also acknowledged this

distinction between "scattered disclosure of the bits of information… and revelation of the [information] as a whole."[xxxvii] Due to this effect, legislation regarding "personally-identifiable information" loses its efficacy because "the data on consumers used in this context is not "personally identifiable" as that term is commonly understood."[xxxviii] This aggregation can provide such a "startlingly complete picture" of an individual, from health, religion, financial circumstances, and relationships, that, in a recently popular case, Target, using only retail transaction data, accurately determined both that a particular consumer was pregnant and the due date for the birth.[xxxix]

Such predictions, which may or may not be accurate, pose risks to individuals beyond simply being intrusive. Marketing algorithms may only provide promotions for higher education or health services to certain demographics of people.[xl] The Podesta report describes the potential for a new application used by the City of Boston and the Mayor's Office of New Urban Mechanics, which allows citizens to report by smartphone the need for city services. As Podesta critiques, "because the poor and the elderly are less likely to carry smartphones or download the Street Bump app, its release could have the effect of systematically directing city services to wealthier neighborhoods populated by smartphone owners".[xli] While the city of Boston has already adjusted the way services are distributed to counter this effect, the potential for unintentional discrimination through data processing will persist.

Data, The Rules

To account for challenges to personal privacy presented by the data industry, current legislation relies on a set of Fair Information Practice Principles (FIPPs), laid out by the Federal Trade Commission in 1973. As delineated by the National Strategy for Trusted Identities in

Cyberspace, these principles include: transparency of motives, encouragement of individual participation, specification of purpose of collection and use, collection of only necessary data, limitations of usage, data quality and integrity, security, and accountability.[xlii] While for the past 40 years these principles, in various forms, have given structure to privacy policy around the world, they fail to properly appease the challenges posed by big data. Companies cannot warn consumers of motives or use of information if data will be sold to a` third party. Individuals cannot be expected to participate in collection of data from every angle with the IoT. Companies cannot be expected to limit data collection when potential for future analysis (often for currently unknown purposes) proves so valuable. These reasons, among others, show that these principles, and the legislation they uphold, must be drastically updated.

The concept of FIPPs originates from a series of studies sponsored by the Department of Health, Education, and Welfare's US Secretary's Advisory Committee on Automated Personal Data System. The resulting 1973 report *Records, Computers, and the Rights of Citizens (*also known as the HEW Report) proposed a "Code for Fair Information Practice" to regulate the "impact of computer-based record keeping on private and public matters," coining the term "Fair Information Practice" (FIP). This code defines four main aspects of personal privacy to outline fair information practice: data record keeping systems cannot be kept secret, an individual must be able to find out what information is recorded and how it is used, the individual must provide consent for information usage, and the individual must be able to "correct or amend" said information.[xliii] While the report stems from and focuses on Social Security Number related privacy breaches, the guidelines that it outlines have been developed and personalized to fit the changing needs of governmental and intergovernmental agencies around the world for the past 40 years (Privacy Online 48).

The practices outlined in the HEW Report served as a foundational framework for the Privacy Act of 1974.[xliv] Designed by the Office of Management and Budget to regulate Federal agency data collection, this statute attempts to establish fair practice by ensuring that "personal information about individuals collected by Federal agencies is limited to that which is legally authorized and necessary and is maintained in a manner which precludes unwarranted intrusions upon personal privacy."[xlv] The statute outlines a Code of Fair Information Practices (FIP), five principles designed to limit the record-keeping techniques of government "agencies." Because of the specific wording of this statute, the principles only apply to agencies, and not to other government entities, such as courts.[xlvi]

Following the publication of the Privacy Act of 1974, France created La Commission nationale de l'informatique et des libertés (CNIL), New Zealand created a Privacy Commissioner, and Canada, Germany, Norway, Denmark, Austria, and Luxembourg all published legislation following the model of the fair information practices.[xlvii] By 1980, more than a third of the OECD member countries had adopted relevant national legislation.[xlviii] While these frameworks are based upon the FIPPs, the European approach views privacy as "a fundamental human right" and thus imposes "top-down regulation" and "across-the-board rules" to restrict data usage and required user consent.

Conversely, in the United States, legislation attempts to regulate the data industry in "particular contexts" through what Podesta refers to as "a sectoral approach"[xlix] and critics call a "hodgepodge" [l] of constitutional protections, guidelines, federal statutes, state laws, treaties, torts, and other regulatory rules. There is no overarching legislation that protects consumer or citizen privacy; instead "different laws… [regulate] different industries and economic sectors" (587). Podesta claims that, by avoiding broad rules to regulate data usage, this haphazard

structure avoids creating obstacles for economic growth.[li] According to the Internet Policy Task Force's 2012 Green Paper published by the Department of Commerce, this sectoral framework "has facilitated innovation and spurred some of the world's most technologically advanced services, while also providing meaningful privacy protections."[lii] The paper does not provide evidence for the connection between the framework and the development of the "world's most technologically advanced services," nor does it clarify the measurement of success for these privacy protections.

While this framework regulates (to an extent) health information, finance, education, and information about children, the approach, critics claim, "also leaves large areas unregulated, especially at the federal level."[liii] The remaining state laws and torts are "ineffective" at regulating data collection by companies and organizations that operate across state and/or international borders; consequently, such commercial bodies operate "without specific statutory obligations to protect personal data."[liv]

However, according to Daniel J. Solove and Woodrow Hartzog's 2014 publication in the Columbia Law Review, these holes in legislation are indeed regulated, not by statutory legislation but by a system of rapidly developing common law enforced by the Federal Trade Commission. Since April of 1995, when the Congress instructed the Commission to hold a public workshop on Consumer Protection and the Global Information Infrastructure as part of the Bureau of Consumer Protection's Consumer Privacy Initiative, the Commission has been generally considered "the broadest and most influential regulating force on information privacy in the United States."[lv] The Federal Trade Commission Act, which prohibits "unfair and deceptive trade acts or practices in or affecting commerce," allows the Commission to regulate the misuse of consumer data as a "deceptive trade act."[lvi] To ensure that such misuse falls under

this jurisdiction, the Commission's self-proclaimed goal is to "encourage and facilitate effective self-regulation as the preferred approach to protecting consumer privacy online."[lvii] Solove and Hartzog conclude that, while underdeveloped, "the foundations exist to develop this common law" into a "robust privacy regulatory regime" that focuses on consumer expectations, extends independently of company privacy provisions.[lviii]

Data, the Future

This goal of eliminating stakeholders from the development of privacy legislation echoes recommendations from the Obama Administration's proposition for a Consumer Privacy Bill of Rights, John Podesta's recent Big Data Report, and PCAST's parallel technological report. According Sheila Jasanoff, Professor of Science and Technology Studies at Harvard University, the difficulty in framing the privacy debate stems from the different contexts in which data can be viewed: as property, as common pool resources, and as identity.[lix] To develop fair regulatory practices, then, it is essential that legislators take into account all of the different stakeholders (ie. the owners of the data, those who seek access to data as a resource, and those whose information is part of the datasets) while delineating rights and regulations. If only government entities and data industry leaders develop regulatory framework, consumers and citizens will remain underrepresented, and controversial surveillance, tracking, and discrimination will continue. The total elimination of stakeholders, however, would destroy the purpose of the American sectoral approach to privacy law: encouragement and facilitation of innovative practices. Instead, as the Obama Administration lays out in its 2012 Bill of Rights proposition, companies, privacy and consumer advocates, international partners, State Attorneys General, Federal criminal and civil law enforcement representatives, and academics, all must be included in the discussions and

development of a foundational Consumer Bill of Rights.[lx]

Such a Bill of Rights, as proposed by President Obama, will serve as baseline legislation to cover gaps in Federal Trade Commission regulation, and will be enforced by the Federal Trade Commission if adopted. Having a foundational framework will provide "consistent protections" for citizens and increase consumer trust. A set and overarching framework will also "lower compliance burdens for companies," providing a much more simplistic and accessible explanation of what behavior is or is not appropriate.[lxi] Finally, a transparent set of rights will avoid the trade barrier-like effects of the current sectoral approach by improving interoperability with international trade partners and foreign governments.

To ensure that a this bill of rights will be sustainable as new technologies develop and data usage grows, this Bill of Rights must focus, as PCAST suggests in its May 2014 report to the president, on the uses of the data and not on particular technological solutions. Regulations against wiretapping, for example, often do not include texting or online communications, and are quickly becoming obsolete. The goals of this Bill of Rights must be stated "in terms of intended outcomes", namely the avoidance of specific privacy violations, and the encouragement of creative new uses of big data.

In conclusion, the new frontier of the data industry demands regulatory interference. Legislators must find a balance between promoting privacy and ensuring consumer rights, and encouraging and facilitating innovation and growth. Privacy and innovation are not at odds; a stronger and more structured set of regulations on the data industry will, if constructed properly, allow for faster growth and safer consumers. An overarching consumer bill of rights, relevant to all government and private sector entities, will fulfill this purpose and secure the nation's future as a leader in innovation and citizen-consumer rights.

Works Cited

"Data, Data Everywhere." *The Economist*, February 27, 2010. Accessed May 5, 2014. http://www.economist.com/node/15557443?story_id=15557443.

Dempsey, James X., and Lara M. Flint. "Commercial Data and National Security." *The Center for Democracy and Technology,* November 3, 2004. https://www.cdt.org/files/publications/200408dempseyflint.pdf.

The Economic Intelligence Unit, "The Deciding Factor: Big Data & Decision Making," *Capgemini*, June 4, 2012. http://www.capgemini.com/resource-file-access/resource/pdf/The_Deciding_Factor__Big_Data___Decision_Making.pdf.

Epsilon Sys. "Internet of Things." Accessed May 5, 2014. http://www.epsilonsys.com/web/we-do/internet_of_things/en/4.html.

Evans, Dave. "The Internet of Things How the Next Evolution of the Internet Is Changing Everything." Rep. *Cisco IBSG,* April 2011. Accessed May 5, 2014. http://www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf.

Ferber, Stefan. "How the Internet of Things Changes Everything." *Harvard Business Review*, May 7, 2013. Accessed May 5, 2014. http://blogs.hbr.org/2013/05/how-the-internet-of-things-cha.

Gambs, Sebastien. "Show Me How You Move and I Will Tell You Who You Are." *Transactions on Data Privacy 4* (2011): 103-26. Accessed May 5, 2014. http://www.tdp.cat/issues11/tdp.a078a11.pdf.

Holdren, John P. "PCAST Releases Report on Big Data and Privacy." *The White House Blog.* 1 May 2014. Accessed May 1, 2014. http://www.whitehouse.gov/blog/2014/05/01/pcast-releases-report-big-data-and-privacy.

IBM. "Bringing Big Data to the Enterprise." Accessed May 5, 2014. http://www-01.ibm.com/software/data/bigdata/what-is-big-data.html.

Lemos, Robert. "Where's the Next Heartbleed Bug Lurking?" *MIT Technology Review,* April 29, 2014. Accessed May 5, 2014. http://www.technologyreview.com/news/527016/wheres-the-next-heartbleed-bug-lurking/.

Lennon, Mike. "Massive Breach at Epsilon Compromises Customer Lists of Major Brands." *Security Week,* April 2, 2011. Accessed May 5, 2014. http://www.securityweek.com/massive-breach-epsilon-compromises-customer-lists-major-brands.

Manyika, James, Michael Chui, Brad Brown, Jacques Bughin, Richard Dobs, Charles Roxburgh, and Angela Hung Byers. *Big Data: The Net Frontier for Innovation, Competition, and Productivity.* McKinsey: 2011.

OECD. "Thirty Years Later: The OECD Privacy Guidelines," 2011. Accessed May 5, 2014. http://www.oecd.org/sti/ieconomy/49710223.pdf.

Privacy Act of 1974, 5 U.S.C. § 552a (2000). Accessed May 5, 2014. http://www.justice.gov/opcl/privstat.htm.

Rivera, Janessa. "Gartner Says the Internet of Things Installed Base Will Grow to 26 Billion Units By 2020." *Gartner,* December 12, 2013. Accessed May 5, 2014. http://www.gartner.com/newsroom/id/2636073.

Russell, Kyle. "Here's How To Protect Yourself From The Massive Security Flaw That's Taken Over The Internet." *Business Insider.* April 8, 2014. Accessed May 5, 2014.

http://www.businessinsider.com/heartbleed-bug-explainer-2014-4#!H2XU4.
Singer, Natasha. "Mapping, and Sharing, the Consumer Genome." *The New York Times*, June 16, 2012. Accessed May 5, 2014. http://www.nytimes.com/2012/06/17/technology/acxiom-the-quiet-giant-of-consumer-database-marketing.html.
Solove, Daniel J., and Woodrow Hartzog. "The FTC and the New Common Law of Privacy." *The Columbia Law Review* 114.3 (2014): 587. April 2014. Accessed May 5, 2014. http://columbialawreview.org/wp-content/uploads/2014/04/Solove-Hartzog.pdf.
Solove, Daniel J. *The Digital Person: Technology and Privacy in the Information Age.* New York: New York UP, 2004. 55. Print.
Tene, Omer, and Jules Polonetsky. "Big Data for All: Privacy and User Control in the Age of Analytics." *Northwestern Journal of Technology and Intellectual Property* 11.5 (2013): 240-73. Web.
U.S. Department of Commerce. Internet Policy Task Force. "Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework." By Gary Locke. S.l.: Bibliogov, 2013. Print.
U.S. Department of Health, Education, and Welfare. "Records, Computers and the Rights of Citizens: Summary and Recommendations." Accessed May 5, 2014. http://epic.org/privacy/hew1973report/Summary.htm.
U.S. Executive Office of the President. "Big Data and Privacy: A Technological Perspective. President's Council of Advisors on Science and Technology." May 1, 2014. Accessed May 5, 2014. http://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdf.
U.S. Executive Office of the President. "Big Data: Seizing Opportunities, Preserving Values." By John Podesta, May 1 2014. Accessed May 5, 2014. http://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf.
U.S. Federal Trade Commission. *Federal Trade Commission Act Section 5: Unfair or Deceptive Acts or Practices*. June 2008. Accessed May 5, 2014. http://www.federalreserve.gov/boarddocs/supmanual/cch/ftca.pdf.
U.S. Federal Trade Commission. "Internet of Things Workshop." MS. Washington, DC, November 19, 2013. Accessed May 5, 2014. http://www.ftc.gov/sites/default/files/documents/public_events/internet-things-privacy-security-connected-world/final_transcript.pdf.
U.S. Federal Trade Commission. *Privacy Online: A Report to Congress*. June 1998. Accessed May 5, 2014. http://www.ftc.gov/sites/default/files/documents/reports/privacy-online-report-congress/priv-23a.pdf.

U.S. Federal Trade Commission. "Protecting Consumer Privacy in an Era of Rapid Change." March 2012. http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.
U.S. National Strategy for Trusted Identities in Cyberspace. "Appendix A – Fair Information Practice Principles (FIPPs)." Accessed May 5, 2014. http://www.nist.gov/nstic/NSTIC-FIPPs.pdf.

U.S. Senate Committee on Commerce, Science, and Transportation Office of Oversight and Investigations. “A Review of the Collection and Sale of Consumer Data for Marketing Purposes.” December 18, 2013. Accessed May 5, 2014. http://www.commerce.senate.gov/public/?a=Files.Serve&File_id=0d2b3642-6221-4888-a631-08f2f255b577.

U.S. Senate Department of Commerce. National Institute of Standards and Technology. “Guide to Protecting the Confidentiality of Personally Identifiable Information (PII).” By Erika McCallister, Tim Grance, and Karen Scarfone. April 2010. Accessed May 5, 2014. http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf.

Wasik, Bill. "In the Programmable World, All Our Objects Will Act as One Gadget Lab WIRED." *Wired,* May 12 2013. Accessed May 5, 2014. http://www.wired.com/2013/05/internet-of-things-2/.

The White House. “Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy.” February 2012. Accessed May 5, 2014. http://www.whitehouse.gov/sites/default/files/privacy-final.pdf.

Wicker, Stephen, and Robert Thomas. "A Privacy-Aware Architecture For Demand Response Systems." Cornell U, n.d. Accessed May 5, 2014. http://www.science.smith.edu/~jcardell/Courses/EGR328/Readings/WickerThomas_HICSS.pdf.

---

[i] “Bringing Big Data to the Enterprise,” IBM, accessed May 5, 2014, http://www-01.ibm.com/software/data/bigdata/what-is-big-data.html.

[ii] James Manyika, “Big data: the net frontier for innovation, competition, and productivity,” *McKinsey & Company*, June 2011, http://www.mckinsey.com/insights/business_technology/big_data_the_next_frontier_for_innovation.

[iii] “The Deciding Factor:Big Data & Decision Making,” *Capgemini,* June 4, 2012, http://www.capgemini.com/resource-file-access/resource/pdf/The_Deciding_Factor__Big_Data___Decision_Making.pdf.

[iv] U.S. Senate, Committee on Commerce, Science, and Transportation, Office of Oversight and Investigations, *A Review of the Data Industry: Collection and Sale of Consumer Data for Marketing Purposes,* December 18, 2013, http://www.commerce.senate.gov/public/?a=Files.Serve&File_id=0d2b3642-6221-4888-a631-08f2f255b577.

[v] Dave Evans, “The Internet of Things: How the Next Evolution of the Internet is Changing Everything,” *Cisco ISBG,* April 2011, http://www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf.

[vi] Janessa Rivera, “Gartner Says the Internet of Things Installed Base Will Grow to 26 Billion Units By 2020,” *Gartner,* December 12, 2013, http://www.gartner.com/newsroom/id/2636073.

[vii] “The Internet of Things: the next big Thing that will change our lives,” Epsilon Sys, accessed May 4, 2014, http://www.epsilonsys.com/web/we-do/internet_of_things/en/4.html.

[viii] Dave Evans, “The Internet of Things.”

[ix] Gambs, “Show Me How You Move and I Will Tell You Who You Are,” 2011, http://www.tdp.cat/issues11/tdp.a078a11.pdf.

[x] Bill Wasik, “In the Programmable World, All Our Objects Will Act as One,” *Wired*, May 14, 2013, http://www.wired.com/2013/05/internet-of-things-2.

[xi] Dave Evans, http://www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf

[xii] Stefan Ferber, “How the Internet of Things Changes Everything,” *Harvard Business Review,* May 7, 2013, http://blogs.hbr.org/2013/05/how-the-internet-of-things-cha/.

[xiii] “A Review of the Data Industry,” 28.

[xiv] “Data, Data, Everywhere,” *The Economist,* May 5, 2010, http://www.economist.com/node/15557443?story_id=15557443.

[xv] Rivera, “Gartner Says.”

[xvi] “Big Data: Seizing Opportunities, Preserving Values,” U.S. *Executive Office of the President,* May 2014, http://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf.

[xvii] Ibid.

[xviii] "Big Data and Privacy: A Technological Perspective," *U.S. Executive Office of the President,* May 2014, http://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdf.

[xix] John P. Holdren, "PCAST Releases Report on Big Data and Privacy," *Office of Science and Technology Policy,* May 1, 2014, http://www.whitehouse.gov/blog/2014/05/01/pcast-releases-report-big-data-and-privacy.

[xx] "Big Data and Privacy: A Technological Perspective."

[xxi] *Internet of Things Workshop,* transcript, U.S. Federal Trade Commission, November 19, 2013, http://www.ftc.gov/sites/default/files/documents/public_events/internet-things-privacy-security-connected-world/final_transcript.pdf.

[xxii] Stephen Wicker, "A Privacy-Aware Architecture For Demand Response Systems," *Cornell University* http://www.science.smith.edu/~jcardell/Courses/EGR328/Readings/WickerThomas_HICSS.pdf.

[xxiii] "A Review of the Data Industry," 30.

[xxiv] "Protecting Consumer Privacy in an Era of Rapid Change," *U.S. Federal Trade Commission,* March 2012, http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

[xxv] "A Review of the Data Industry," 32.

[xxvi] Ibid., 28.

[xxvii] Ibid., 32.

[xxviii] Ibid., 32.

[xxix] Robert Lemos, "Where's the Next Heartbleed Lurking?," MIT Technology Review, APril 29, 2014, http://www.technologyreview.com/news/527016/wheres-the-next-heartbleed-bug-lurking.

[xxx] Kyle Russell, "Here's How To Protect Yourself From The Massive Security Flaw That's Taken Over The Internet," *Business Insider*, April 8, 2014, http://www.businessinsider.com/heartbleed-bug-explainer-2014-4#!H2XU4.

[xxxi] "Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)," *U.S. Department of Commerce, National Institute of Standards and Technology,* April 2010, http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf.

[xxxii] Omer Tene, "Big Data for All: Privacy and User Control in the Age of Analytics," *Northwestern Journal of Technology and Intellectual Property* (2013): 240-73.

[xxxiii] Mike Lennon, "Massive Breach at Epsilon Compromises Customer Lists of Major Brands," *Security Week,* April 2, 2011, http://www.securityweek.com/massive-breach-epsilon-compromises-customer-lists-major-brands.

[xxxiv] Natasha Singer, "Mapping, and Sharing, the Consumer Genome," *The New York Times,* May 5, 2011, http://www.nytimes.com/2012/06/17/technology/acxiom-the-quiet-giant-of-consumer-database-marketing.html.

[xxxv] "Protecting Consumer Privacy in an Era of Rapid Change."

[xxxvi] Daniel J. Solove, *The Digital Person: Technology and Privacy in the Information Age* (New York, New York: UP 2004), 55.

[xxxvii] James X. Dempsey, "Commercial Data and National Security," 2004.

[xxxviii] " A Review of the Data Industry."

[xxxix] "Protecting Consumer Privacy in an Era of Rapid Change."

[xl] Natasha Singer, "Mapping and Sharing the Consumer Genome," *The New York Times,* July 16, 2012, http://www.nytimes.com/2012/06/17/technology/acxiom-the-quiet-giant-of-consumer-database-marketing.html.

[xli] "Big Data: Seizing Opportunities, Preserving Values."

[xlii] "Appendix A – Fair Information Practice Principles (FIPPs)," U.S. National Strategy for Trusted Identities in Cyberspace, http://www.nist.gov/nstic/NSTIC-FIPPs.pdf.

[xliii] U.S. Department of Health, Education, and Welfare, *Records, Computers and the Rights of Citizens: Summary and Recommendations,* http://epic.org/privacy/hew1973report/Summary.htm.

[xliv] U.S. Department of Justice, *The Privacy Act of 1974*, http://www.justice.gov/opcl/privstat.htm.

[xlv] U.S. Department of Commerce, Internet Policy Task Force, *Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework,* December 2010.

[xlvi] Ibid.

[xlvii] "Thirty Years Later: The OECD Privacy Guidelines," *OECD,* http://www.oecd.org/sti/ieconomy/49710223.pdf.

[xlviii] Ibid.

[xlix] "Big Data: Seizing Opportunities, Preserving Values."

[l] Daniel J. Solove, "The FTC and the New Common Law of Privacy," *The Columbia Law Review*, April 2014, 587, http://columbialawreview.org/wp-content/uploads/2014/04/Solove-Hartzog.pdf.

[li] "Big Data: Seizing Opportunities, Preserving Values."

[lii] "Commercial Data Privacy," 11.

[liii] Solove, 587.

[liv] "Commercial Data Privacy," 12.

[lv] U.S. Federal Trade Commission, *Privacy Online: A Report to Congress,* http://www.ftc.gov/sites/default/files/documents/reports/privacy-online-report-congress/priv-23a.pdf (June 1998); Solove,, 586.

[lvi] U.S. Federal Trade Commission, *Federal Trade Commission Act Section 5: Unfair or Deceptive Acts or Practices,* http://www.federalreserve.gov/boarddocs/supmanual/cch/ftca.pdf.

[lvii] Ibid.

[lviii] Solove, 586.

[lix] "Big Data: Seizing Opportunities, Preserving Values."

[lx] The White House, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy,* February 2012, http://www.whitehouse.gov/sites/default/files/privacy-final.pdf.

[lxi] Ibid.