Testimony of Pam Dixon
Executive Director, World Privacy Forum

Before the US Senate Committee on the Judiciary, Subcommittee on Privacy, Technology, and the Law

Data Brokers — Is Consumers' Information Secure?

November 3, 2015

Chairman Flake and Members of the Committee, thank you for the opportunity to testify today about data brokers and the security of the information they acquire, store, analyze, and transmit. This is an industry largely hidden from public view, and I appreciate your efforts to shed light on these issues.

I am Pam Dixon, founder and Executive Director of the World Privacy Forum.[1] The World Privacy Forum is a 501(c)(3) non-partisan public interest research group based in California. We focus on conducting in-depth research on emerging and contemporary privacy issues as well as consumer education.

I have been conducting privacy and security-related research since 1998, first as a Research Fellow at the Denver University School of Law's Privacy Foundation, where I researched technology-related privacy issues. While a Fellow, I had the privilege of working with Richard M. Smith, the noted security expert, and wrote the first longitudinal research study benchmarking data flows in employment online and offline.

After founding the World Privacy Forum, I researched and wrote about privacy and commented on numerous regulatory proposals affecting privacy and security. The WPF also created useful, practical education materials for consumers. Most recently, I researched and co-authored with Robert Gellman several pathbreaking reports. The most recent is a report about data analytics, *The Scoring of America: How secret consumer scores threaten your privacy and your future.*[2]

---

[1] www.worldprivacyforum.org.

[2] https://www.worldprivacyforum.org/2014/04/wpf-report-the-scoring-of-america-how-secret-consumer-scores-threaten-your-privacy-and-your-future/.

This report documents for the first time extensive consumer analytics activities and products that were hidden from public view. We also published a report on data brokers and the Federal government, *Data Brokers and the Federal Government*,[3] examining current law and practices about the use of data brokers in federal programs.

The WPF also produced many additional studies. In 2005, I discovered previously undocumented consumer harms related to identity theft in the health sector. I coined a term for this activity: medical identity theft. In 2006, I published a groundbreaking report introducing and documenting the topic of medical identity theft. The report remains the definitive work in the area.[4] In 2010, I published the first report on digital and retail privacy, *The One Way Mirror Society: Privacy Implications of Digital Signage Networks*.[5] I also wrote and co-authored several well-known reports on self-regulation such as *The Network Advertising Initiative: Failing at Consumer Protection and at Self Regulation*,[6] and *Many Failures: A brief history of privacy self regulation*.[7]

Beyond my research work, I co-authored a reference book on privacy, *Online Privacy*, and wrote seven books on technology issues with Random House, Peterson's and other large publishers, as well as more than one hundred articles in newspapers, journals, and magazines. Most recently, I edited a two-volume reference on Surveillance which will appear in 2016.

I appreciate the work of Senator Flake and this Subcommittee in bringing much-needed attention to the issue of data broker security, a topic infrequently discussed but of great importance.

---

[3] https://www.worldprivacyforum.org/2013/10/report-data-brokers-and-government-introduction-and-background/.

[4] Dixon, Pam. *Medical Identity Theft: The information crime that can kill you*, World Privacy Forum, May 2006. https://www.worldprivacyforum.org/2006/05/report-medical-identity-theft-the-information-crime-that-can-kill-you/.

[5] Dixon, Pam and Gellman, Robert. *The One-Way Mirror Society, Privacy implications of the new digital signage networks*, January 2010. https://www.worldprivacyforum.org/2010/01/report-one-way-mirror-society/.

[6] https://www.worldprivacyforum.org/2007/11/report-nai-failing-at-consumer-protection-and-at-self-regulation/.

[7] https://www.worldprivacyforum.org/2011/10/report-many-failures-a-brief-history-of-privacy-self-regulation/, Robert Gellman, lead author.

Introduction

It is no longer sustainable for data brokers[8] of any size to handle high volumes of sensitive and detailed consumer data in the absence of minimum national data security standards. As the acquirers, transmitters, storers, and analyzers of consumer data in volumes that rival the largest US commercial sectors, data brokers have grown in importance and prominence to such a degree that it is unthinkable that such an integral part of the economy would remain unregulated as to security standards. The risks are too great.

Fortunately, we do not need to reinvent the wheel here. Other sectors already have minimum national security standards, including the health, financial, education, governmental sectors. These standards have created a clear pathway of security improvement, and now suggest a roadmap for establishing minimum security standards for data brokers.

Years of careful thought and discussion went into developing the HIPAA health data security standard — a national standard that applies to all HIPAA-covered entities. The flexibility and scalability of the HIPAA security standard allowed it to be deployed in a wide range of businesses and across highly complex business structures and variables. Similarly, FISMA, Gramm-Leach-Bliley, and FERPA brought sustainable security practices to major sectors of the US economy.

Although it is inevitable that data breaches and lapses happen, they happen far less often than would have been the case if robust and yet reasonable security standards were not in place. It is unreasonable and insecure to allow data brokers to continue to do business using consumer and other data without minimum national security standards in place.

Data brokers hold extraordinary stores of sensitive and other data, some of which is extremely alluring to criminals. Data brokers are one of the ultimate data-rich targets, with data ranging from biometric data to health data to criminal data to background check data to financial data to transactional data and much more. In its report on Data Brokers, the Federal Trade Commission noted that data brokers' lengthy storage of consumer data can create security risks.[9] It is quite possible that the files of data brokers contain much of the same personal information as the Office of Personnel Management that was recently the target of a successful hack by a foreign nation.

---

[8] I am using the FTC definition of data brokers found in its report, *Data Brokers: A call for Transparency and Accountability*, May 2014. https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf

[9] Id, p. vi. From the FTC Data Broker report: "For example, identity thieves and other unscrupulous actors may be attracted to detailed consumer profiles maintained by data brokers that do not dispose of obsolete data, as this data could give them a clear picture of consumers' habits over time, thereby enabling them to predict passwords, answers to challenge questions, or other authentication credentials."

Risks to consumers from data breaches are well-known, and include identity theft, fraud, and more. Members of law enforcement, state and federal judges, and Members of Congress face the same risks. There are other risks as well because information held by data brokers may be breached and sold on the dark web, where fraudsters purchase it and use it to apply for loans, harming both the individual consumer and defrauding businesses. This activity creates a drag on the national economy.

Data brokers collect, store, analyze, and transmit data nationally and in some cases globally. Their databases contain highly detailed and sometimes longitudinal consumer information. This sector remains unregulated for security practices, while similar data held by health practitioners, banks, and federal agencies is subject to security rules. It is time for Congress to bring good security standards to the data broker sector.

Scope, Breadth, and Depth of Data Broker Data

Data brokers hold more data about Americans than the US government does. As major contractors to the US government, a variety of law enforcement agencies, the financial sector, the education sector, the health care sector, the retail sector, and insurance companies, data brokers regularly process data that in other contexts would be regulated. Data brokers collect information, transmit information, analyze and categorize information, and store information, among other activities. It is important to fully understand the scope, breadth, and depth of data broker data, and to see that the same data regulated in one context can readily flow into data broker files where it loses its regulation — and where consumers lose the protections that they formerly enjoyed.

Data brokers obtain consumer data from many sources: public data, privately purchased or custom data, lists of data from other data brokers, retail transaction records, social scores, census tract data, lifestyle and other types of consumer patterns, health conditions, ethnicity, book purchasing patterns, exercise patterns, and more. Data broker information used may be individual to one consumer or modeled (e.g., all consumers in a census tract).

Some still believe that data brokers primarily sell lists. That is no longer the case for the larger and more sophisticated data brokers. Instead, data brokers view data as a commodity, and focus more on data analytics using copious amounts of unregulated data, and sometimes a mix of regulated and unregulated data. Data brokers are typically complex companies with multiple lines of business models, and highly complex national and sometimes multinational data flows. Occasionally, a data broker may engage in an activity that fall under some regulatory control, but more of their data processing is subject to little to no restrictions on use, sale, or maintenance.

To make clear the wide range of data that data brokers traffic in, I include here a list of the most common elements of consumer data available today. Most consumers would be stunned to learn the amount of data available about them in the commercial marketplace. While regulations covering data such as health data provide data subjects with rights and consumer choice, data brokers generally have no obligation to data subjects in the area of unregulated data.

This list is excerpted from *The Scoring of America* report and includes independent data sets with both structured and unstructured data. This list is sourced in part from 2015 research, as well as the 2013 Government Accountability Office Report on information resellers. Other information came from a WPF review and analysis of data broker data cards viewed through public Internet sources over the course of a year (primarily 2013), and also from WPF review and analysis of reliable data broker and analytics web sites that list data sources.[10] For example, the Acxiom About the Data portal lists many categories of information collected and used for consumer marketing.[11]

The data sets available for purchase today listed here – along with others we did not identify – can create multiple layers of predictive analysis of how consumer behavior, finance, demographics, geography, and the other factors listed here interact. That does not necessarily mean that the results are better.

Data broker data can include:

Demographic and other identifying Information:
- Age
- Age range
- Date of birth
- Biometric data, for example, voice print or face print
- Education
- Exact date of birth
- Gender
- Marital status
- Home ownership
- Own or rent
- Estimated income
- Exact income
- Ethnicity
- Presence of children
- Number of children

---

[10] MyFico, "Credit Education," <http://www.myfico.com/CreditEducation/>.

[11] Acxiom, About the Data Portal, https://aboutthedata.com/portal/registration/step1.

• Age range of children
• Age of children
• Gender of children
• Language preference
• Religion
• Occupation - category of occupation
• Examples: Beauty (cosmetologists, barbers, manicurists) civil servants, clergy, clerical/office workers, doctors/physicians/surgeons, executives/administrators, farming/ agriculture, health services, middle management, nurses, professional/technical, retail service, retired, sales, marketing, self-employed, skilled/trade/machine operator/laborer, teacher/educator.
• Occupation - title of occupation
• Military history
• Veteran in household
• Voter party
• Professional certificates (teacher, etc.)
• Education level reached or median education

Contact Information:
• Full name
• Email address
• City
• State
• ZIP
• ZIP + 4
• Home Address
• Land-line phone
• Social IDs / social media handles and aliases
• Mobile phone number
• Carrier
• Device type
• Email address

Vehicles:
• Vehicle make, model and year
• VIN
• Estimated vehicle value
• Vehicle lifestyle indicator
• Model and brand affinity
• Used vehicle preference indicator

Lifestyle, Interests and Activities data (including medical):
• Antiques
• Apparel (women, men & child)

• Art
• Average direct mail purchase amounts
• Museums
• Audio books
• Auto parts, auto accessories
• Beauty and cosmetics
• Bible purchaser
• Bird owner
• Books
• Book purchases - plus types. (Mystery, romance, religious, etc.)
• Book clubs
• Career
• Career improvement
• Cat owner
• Charitable giving indicators:
• Charitable donor by type of donation (religious, health, social justice)
• Charitable donor by ethnicity or religion (Jewish donors, Christian donors, Hispanic donors)
• Charitable donor by financial status (wealthy donors)
• Children or teen interests
• Fashion and clothing (Multiple: sports, high fashion, shoes, accessories, etc.)
• Collectibles
• Collector
• Christian families
• Computer games
• Computers
• Consumer electronics (Many categories, including electronic fitness devices)
• Dieting and weight loss
• Telecommunications and mobile
• Dog owner
• Investing
• DVD purchasers
• Electronics - home, computing, office, other
• Empty nester
• Expectant parents
• Frequent mail order buyer
• Frequency of purchase indicator
• Getting married
• Getting divorced
• Gun ownership
• Health and beauty
• Health and medical: for example, Allergies, Alzheimer's disease, angina,

arthritis/rheumatism, asthma, back pain, cancer, clinical depression, diabetes, emphysema, erectile dysfunction, epilepsy, frequent heartburn, gum problems, hearing difficulty, high blood pressure, high cholesterol, irritable bowel syndrome, lactose intolerant, ulcer, menopause, migraines/frequent headaches, multiple sclerosis, osteoporosis, Parkinson's disease, prostate problems, psoriasis/eczema, sinusitis/sinuses. Some data is direct, some inferred.

- High-end appliances
- Home improvement
- Household consumer expenditures — many categories.
- Jewelry
- Magazine subscriptions
- Mail order buyer
- Mobile location data (some analytics companies)
- Movies - attendance / collector
- Musical instruments
- Music
- New mover
- New parent
- Online and continuing education
- Online purchasing - many categories
- Parenting
- Pets - other
- Plus size clothing purchase
- Political affiliation
- Recent home buyer
- Recent mortgage borrower
- Retail purchasing - many categories.
- Science-related
- Sexual orientation
- Social media sites likely to be used by an individual or household, heavy or light users
- Spa
- Sports interests: (large category, these are examples)
- Birdwatching
- Equestrian
- Exercise and fitness
- Gardening
- Golf
- Fishing
- Outdoor interests - hiking, camping, climbing
- Swimming, diving, snorkeling
- Spectator Sports
- Stamps/coins
- Yoga

• Television, Cable, Satellite/Dish
• Travel: Vacations, domestic and/or international
• Purchase of international hotel or air flights
• Frequent flyer
• Types of purchases indicator
• Veteran in household
• Vitamins
• Volunteering

Financial and Economic – Property and Assets data:
• Estimated income
• Estimated household income
• Home value
• Length of residence
• Payment data: 30, 60, 90-day mortgage lates
• Purchase date
• Purchase price
• Purchase amount
• Most recent interest rate type
• Most recent loan type code
• Sales transaction code
• Most recent lender code
• Purchase lender code
• Most recent lender name
• Purchase lender name
• Fuel source
• Loan to value
• Purchase interest rate type
• Most recent interest rate
• Purchase interest rate
• Pool or spa
• Home - year built
• Air conditioning
• Boat ownership
• Plane ownership
• Motorcycle ownership
• Commercial assets or business ownership

Financial and Credit data:
• Bankruptcy
• Beacon score
• Credit score - actual
• Certificates of deposit/ money market funds

• Estimated household income ranges
• Income producing assets indicator
• Estimated net worth ranges
• IRAs
• Life insurance
• Low-end credit scores
• Mutual funds/annuities
• Summarized credit score or modeled credit score by neighborhood
• Payday loan purchaser
• Number of credit lines
• Tax liens
• Card data:
• Card holder - single card holder
• Range of new credit
• Debit or credit card present in household
• Card holder - brand (Discover, Visa, Mastercard, etc.)
• Card holder - type (Gas, bank, premium, luxury, prepaid, etc.)
• Frequent credit card user
• New retail card holders
• Underbanked or "thin file"
• Stocks or bonds
• Average online purchase
• Average offline purchase

In addition, a business may give data brokers enterprise data (historic data from its own customer files) to create proprietary analyses for the business' internal use. Note that some data is direct data, some data is inferred. Taken a single data elements, the information that data brokers hold may not seem extraordinary. However, it is not just about the data itself. The stakes here also include the data compilations, overlays, analyses, and transformations. Typically, "consumer scores" can be crafted from this data, these become rich sources of customer insight and analytics — for businesses. Unlike the regulated credit score, most consumer scores are totally hidden from consumers, who have no redress or protections.

Regulation of Data Security in other Sectors— and the Lack of National Data Broker Security Standards

Significant sectoral data collections are subject to federal security standards. These sectors include health, finance, government, and education, among others.[12] Yet data brokers — despite the voluminous and sensitive information they collect, store, and transmit — are not subject to similar national minimum security standards. Sometimes the same data that is regulated, when

---

12

stored by data brokers, is not regulated because it is not used for the same purposes as regulated data.

Data broker clients include the federal government, states, cities, law enforcement, academic institutions, employers, students, researchers, and other individuals. In many cases, these same clients are also data sources. Governments at all levels buy information from government agencies and then sell the same information, enhanced with data rom other sources, back to the same agencies. Data broker activities form an extraordinary data exchange across the nation and across the globe. It is worth observing that data brokers that function in Canada, Europe, and many other countries around the world are subject to privacy and security standards. These companies function profitably in these environments, notwithstanding the privacy and security rules. There is no reason why data brokers cannot be both successful and regulated here in the United States.

Here are some of the most significant and relevant standards that are operative in other US sectors today:

Health Insurance Portability and Accountability Act (HIPAA) Security Rule

The HIPAA Security Rule covers protected health information held by HIPAA-covered entities, and requires that covered entities under the rule conduct a risk assessment of their healthcare organization. The definition of protected health information (PHI) under the HIPAA Privacy Rule covers protected health information in any medium, paper, digital, or otherwise. The definition of PHI under the HIPAA Security Rule encompasses electronic protected health information, often called "EPHI."

The HIPAA Security Rule sets national security standards for protecting EPHI in three areas: administrative, physical, and technical safeguards. The standards apply to individuals' electronic personal health information (EPHI) that is either created, received, used, or maintained by a HIPAA-covered entity. The security standards are technology neutral — they do not mandate the use of specific security technologies or methods.[13]

---

[13] While it is beyond the scope of this testimony to cover the HIPAA Security Rule in detail, I would like to briefly mention how the key safeguards interact:

> Administrative safeguards: Administrative functions are the practical steps and delegations of authority and operations that covered entities should implement in order to meet the security standards. Security training of personnel is an example of this. (45 CFR § 164.308.)
> Physical safeguards: These safeguards are to protect digital systems and data from threats, whether those be unauthorized intrusions or environmental hazards such as destruction from events such as hurricanes. This category of safeguards include restricting access to digital protected health information and retaining off-site computer backups. (45 CFR § 164.310.)
> Technical safeguards: These are safeguards to protect data and control access to data. They include using authentication controls to verify access to protected data, and encrypting and decrypting data as it is being stored and/or transmitted. (45 CFR § 164.312.)

Gramm-Leach Bliley Act (GLBA) Data Safeguard Rules

The GLBA Safeguard Rule[14] is a financial regulation that requires entities covered under its regime to provide privacy notices and to limit information sharing in particular ways.[15] For example, to limit information sharing to non-affiliated businesses in certain conditions. This area of financial regulation has been intensively studied, and plentiful documentation exists regarding how much budget implementation costs.[16]

Family Educational Rights and Privacy Act (FERPA)

FERPA applies to educational records held by educational institutions. Educational records can include student financial aid information, grades, and in some cases may include health treatment information. FERPA is a complex statute in its interactions with HIPAA. Nevertheless, FERPA sets prohibitions on the disclosure of students' educational records, with various loopholes, but also requirements that must be met prior to disclosures.

In recent years, longitudinal reporting of aggregate school record data has come under questioning based on re-identifiability of aggregate student records subject to FERPA controls. The educational sector has conducted extensive statistical de-identification work in this area.[17]

Sarbanes-Oxley

Sarbanes-Oxley (SOX) contains important risk management and internal control requirements.[18] These requirements ensure that businesses understand and have adequate internal controls, including of business processes and data. The risk assessment and internal control procedures in

---

[14] https://www.ftc.gov/tips-advice/business-center/guidance/financial-institutions-customer-information-complying

[15] CFPB Examination Manual: http://files.consumerfinance.gov/f/201210_cfpb_supervision-and-examination-manual-v2.pdfGLBA, Regulation P
"GLBA and Regulation P govern the treatment of nonpublic personal information about consumers by financial institutions and restrict the sharing of nonpublic personal information with unaffiliated third parties. GLBA requires financial institutions to disclose their privacy policies to consumers. GLBA also permits consumers to opt out of certain sharing practices.
1. Determine whether the entity's information sharing practices are consistent with the requirements of the GLBA and implementing rule. Please refer to the examination procedures regarding Regulation P, 12 CFR 1016.4, for more information."

[16] http://files.consumerfinance.gov/f/201311_cfpb_report_findings-relative-costs.pdf

[17] National Institute of Statistical Sciences (NISS) Data Confidentiality Technical Panel Report http://nces.ed.gov/pubsearch/pubsinfo.asp?pubid=2011608

[18] http://www.sec.gov/about/laws/soa2002.pdf and http://www.sec.gov/spotlight/soxcomp.htm.

Section 404 apply across a broad swath of organizational entities. SOX has much applicability to access controls.[19]

Other security regulations exist, however my focus here is on complex national security regulation of large data collections. Data brokers have many points of comparison with the existing sectoral national security standards, and much can be learned from understanding the flexible, technology-neutral yet protective standards approach that for example the HIPAA Security Rule have taken.

Examples of data broker security clauses

In some cases, data brokers publish Terms of Service or Terms of Use for small business products publicly. I have included two such examples by Experian and Acxiom. These are security clauses that are available for data products, and the security clauses are contained within a larger set of Terms. The data brokers likely have multiple other sets of Terms for other products.

Experian Small Business security clause:

> (d) You will maintain reasonable security procedures and practices appropriate to the nature of the information to protect the Experian Data from unauthorized access, destruction, use, modification or disclosure. You shall provide Experian immediate written notice upon discovery or notification of any Security Breach and immediately and at Your own expense investigate and take all steps to identify, prevent and mitigate the effects of any Security Breach. You shall promptly provide to Experian a detailed description of the incident, the Experian Data accessed, the identity of affected consumers, and such other information as Experian may request concerning the Security Breach and conduct any recovery necessary to remediate the impact and bear any cost or loss Experian may incur as a result of a Security Breach, including any cost associated with Experian notifying any effected consumers.[20]

Acxiom Data Products License Agreement clause

In its Data Products License Agreement for its suite of pay- as- you- go data products, Acxiom includes this statement about security: (“f”)

---

[19] Sarbanes Oxley guidance is at this point mature with robust case studies and history. See, for example, http://www.protiviti.com/en-US/Documents/Resource-Guides/ACE_FAQ_Guide.pdf, p, 18.

[20] Experian Online Data License Terms and Conditions http://www.experian.com/small-business/legal-terms.html.

Customer represents and warrants that: (a) it is a duly formed entity (i.e., corporation or limited liability company) in good standing under the laws of the state of its incorporation or organization; (b) it is qualified to transact business in all states where the ownership of its properties or nature of its operations requires such qualification; (c) it has full power and authority to enter into and perform the Agreement; (d) the execution and delivery of the Agreement have been duly authorized; (e) any Customer Data submitted to Acxiom for processing has been legally obtained and provided to Acxiom; and (f) it maintains an information security program that has administrative, technical, and physical safeguards (that are appropriate for Customer's size and complexity, the nature and scope of Customer's activities, and the sensitivity of Customer's consumer information) sufficient to protect any Confidential Information disclosed to Customer by Acxiom pursuant to this Agreement. Customer further warrants that its use of the Product will be in accordance with all applicable laws and regulations, including Customer's compliance with any applicable registration requirements with state, federal, and other regulatory entities prior to Customer's use of the Product, including but not limited to registration in states for telemarketing purposes as required by each state.[21]

Prior to signing up for this product, Acxiom requests an immediate up-front disclosure regarding HIPAA data, and asks if someone is sending them HIPAA-restricted data.[22]

Sensitive Data

Sensitive data has been broadly outlined and defined by Congress over a long course of time. The Fair Credit Reporting Act, GLBA, HIPAA, the Genetic Information Nondiscrimination Act, the Common Rule and other statutes act to describe the boundaries of "sensitive." Nevertheless, what sensitive data is and is not to data brokers deserves special attention in the context of security, because sensitive information may be encrypted more readily than non-sensitive data, and may be subject to greater security protections.

The difficulties of defining sensitive data outside of the regulatory context are many. In the area of unregulated data, the definition of sensitive data has been hotly debated, most notably in the self-regulatory advertising environment.

Some laws, rules, and policies, both here and abroad, define sensitive data. While many of these efforts are sincere, existing definitions are all different and, to some extent, contradictory. The problem is that it is impossible to define sensitive data without a context. Personal information that seems innocuous in one context may be sensitive in another, and vice versa. No matter how

[21] Acxiom Data Products License Agreement Version: 2014-09.02. the Terms and Conditions are a pop up from the My Acxiom Partner site.

[22] My Acxiom Partner, https://www.myacxiompartner.com/signup.html.

sincere or well-meaning a definition of sensitive information may be, it will create conflicts and problems at some time. Let me give you a few salient examples of why this is so.

Home address: Data brokers typically place public records data as non-sensitive information. I understand the logic behind this. However, victims of crimes, victims of domestic violence, judges, police officers, and jurors are among those individuals for whom a home address is sensitive information.

Medical diagnoses: Some individuals go on Facebook and disclose their health conditions or share their health data through other Internet activities. For these individuals, it can be argued that a publicly discussed condition of cancer or Huntington's Disease is fair game for a data broker collection and is non-sensitive data. However, some diseases have profound genetic implications — such as Huntington's — and implicate the privacy of more than one person. Even after being made public, some health data may be "sensitive" to relatives.

Marital status: Marital status is not generally considered to be sensitive information in most contexts. But in the context of a loan. marital status is protected information under the Equal Credit Opportunity Act, and rules surround the use of this information.

Sensitive information quickly becomes a quagmire of context and subtlety. What is sensitive information in one context, may not be in another, and visa versa. Dr. Helen Nissenbaum of New York University has written and researched context of data extensively, documenting many

subtle aspects of contextual privacy.[23] The White House, in its Consumer Privacy Bill of Rights, included a contextual principle in its statement of consumer rights, Principle 3.[24]

Because it is not possible to produce a clear, workable, and uniform legislative definition of sensitive personal information, we are left with only one option, which is to to treat all personal information as requiring the same level of protection for privacy and security.

I recognize that some will disagree, but it is not a sustainable position for companies to think that they can deliberate somehow to determine that some information is sensitive and some is not. The volume and range of data is simply too large, and the ability of data brokers and others to combine the data in multiple ways makes it impossible to place a tag of "sensitive" on one pile of data or analytics, and not another.

In the interest of security and efficient business processes, the policy of all data as worthy of similar privacy protections and subject to the same security standards makes a great deal of sense and is a good and sustainable path forward. I recognize that this is not a perfect choice. But it is the best and most secure choice, and it is a fair choice. Data brokers should be subject to privacy and security standards just like other businesses and government agencies that process volumes of personal data.

---

[23] H. Nissenbaum, "A Contextual Approach to Privacy Online," *Daedalus* 140 (4), Fall 2011: 32-48. See also A. Barth, A. Datta, J. Mitchell, and H. Nissenbaum, "Privacy and Contextual Integrity: Framework and Applications," Proceedings of the IEEE Symposium on Security and Privacy, May 2006. (Showcased in "The Logic of Privacy," *The Economist*, January 4, 2007.)

[24] CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY, Consumer Privacy Bill of Rights.https://www.whitehouse.gov/sites/default/files/privacy-final.pdf See Principle 3: "RESPECT FOR CONTEXT: Consumers have a right to expect that companies will collect, use, and disclose personal data in ways that are consistent with the context in which consumers provide the data. Companies should limit their use and disclosure of personal data to those purposes that are consistent with both the relationship that they have with consumers and the context in which consumers originally disclosed the data, unless required by law to do otherwise. If companies will use or disclose personal data for other purposes, they should provide heightened Transparency and Individual Control by disclosing these other purposes in a manner that is prominent and easily actionable by consumers at the time of data collection. If, subsequent to collection, companies decide to use or disclose personal data for purposes that are inconsistent with the context in which the data was disclosed, they must provide heightened measures of Transparency and Individual Choice. Finally, the age and familiarity with technol- ogy of consumers who engage with a company are important elements of context. Companies should fulfill the obligations under this principle in ways that are appropriate for the age and sophistication of consumers. In particular, the principles in the Consumer Privacy Bill of Rights may require greater protections for personal data obtained from children and teenagers than for adults."

It is useful to compare several concrete examples of self-regulatory definitions of sensitive data. Included are the definitions from the NAI and the DAA as a direct comparison of sensitive data defined in an advertising self-regulatory context, and a separate sensitive definition by Acxiom.

NAI definition of sensitive data, including health data: [25]

- Sensitive Data
- Sensitive Data includes:
- Social Security Numbers or other government-issued identifiers;
- Insurance plan numbers;
- Financial account numbers;
- Information about any past, present, or potential future health or medical conditions or treatments, including genetic, genomic, and family medical history, based on, obtained, or derived from pharmaceutical prescriptions or medical records, or similar health or meical sources tht provide actual knowledge of a condition or treatment (the source is sensitive);
- information, including inferences, about sensitive health or medical conditions or treatments, including, but not limited to, all types of cancer, mental health-related conditions, and sexually transmitted diseases (the condition or treatment is sensitive regardless of the source); and
- sexual orientation.

DAA definition of sensitive information, including health data:[26]

> Refraining from the Collection of Sensitive Information
>
> You should not collect "personal information," as defined in the Children's Online Privacy Protection Act (COPPA), from children that you have actual knowledge are under the age of 13 or from sites directed to children under the age of 13 for OBA purposes, or engage in OBA directed to children that you have actual knowledge are under the age of 13 except as compliant with the COPPA.
>
> In addition, you should obtain consent before collecting financial account numbers, Social Security numbers, pharmaceutical prescriptions or medical records related to a specific individual for OBA purposes. Consent requires an individual's action in response to a clear, meaningful and prominent notice.

---

[25]NAI Code of Conduct http://www.networkadvertising.org/code-enforcement/code.

[26]DAA Code of Conduct http://www.aboutads.info/principles.

Acxiom defines sensitive data in one of its service agreements as the following:

> Company shall neither provide to Acxiom nor cause Acxiom to use any Sensitive Data for use with the Services. 'Sensitive Data' shall mean: (i) PII related to a data subject under the age of thirteen (13); (ii) Social Security number with the associated name; (iii) mother's maiden name with the associated name; (iv) driver's license or other government issued identification card numbers with the associated name; (v) telephone numbers identified as unlisted or unpublished; (vi) credit, debit card or financial account numbers with the associated name and any required PIN or access code; (vii) personally identifiable payroll/financial information including employee identification numbers; (viii) any data that implicates or is governed by the Fair Credit Reporting Act (aka 'FCRA'); or (ix) personally identifiable health information or any data that implicates or is governed by the Health Insurance Portability and Accountability Act (aka 'HIPAA') or the Health Information Technology for Economic and Clinical Health Act (aka 'HITECH').[27]

Minimum Data Security Requirements: The Practicalities

It is time to set national minimum data security requirements for data brokers. Standards already exist in the financial, health, and technology sectors. The work has been accomplished and due to the appropriate flexibility of the standards, the security practices of each sector continue to evolve in dynamic ways to fit ongoing and ever-changing security challenges.

After working in privacy and security since the 1990s, I have come to the conclusion that the HIPAA approach to security standards is the right overall approach to security regulations in a complex sector. Under the HIPAA approach, health care providers and insurers covered by HIPAA have substantial leeway to determine how to apply security practices to their own particular circumstances. HIPAA covered entities must make choices and document their choices. The documentation provides a good basis for oversight and accountability.

The same type of flexible approach can be used for minimum data broker security standards. Although it is difficult to imagine in a sector as complex and as data-rich as health care without security standards, before the passage of HIPAA, the healthcare sector did not have national minimum security standards for health information. As healthcare organizations and related businesses transitioned from paper to digital files, the need for standards became pressing. The same is now true of data brokers.

---

[27] Acxiom Data Products License Agreement Version: 2014-09.02. My Acxiom Partner, https://www.myacxiompartner.com/signup.html.

Standards

We prefer using the National Institute of Standards and Technology (NIST) as the standards-setting body for security standards for data brokers. As the members of this Subcommittee know, NIST is a federal agency that sets computer security standards for the Federal government. NIST also publishes significant research studies and reports on many aspects of cybersecurity, including work on encryption. While NIST does not always get privacy right, NIST is the right organization for setting security standards, with expertise on security and a history of consultation with all interested parties and the public.

Enforcement

The most significant challenge for a data security standard is enforcement. While the FTC seems a natural and understandable choice for security enforcement for data brokers, the FTC does not have the resources to handle a major new subject. The Commission struggles to do a good job in the areas already within its jurisdiction. Unless Congress is willing to create a much larger FTC with examination authority, I urge a different pathway.

Because the US has set itself along a sectoral path, it is nearly impossible to turn away from that path now. The health sector is already subject to existing and functional security rules under HIPAA. The federal government has its own security rules under Federal Information Security Modernization Act (FISMA). There seems little reason to try to change these existing laws and policies, and it is not clear that any congressional committee has the jurisdiction to change all of these approaches in the same piece of legislation.

For better and worse, the past decisions and regulations have significant impacts on security standards, and there is no reason to change what we already have that works adequately. I favor an approach which has NIST setting the standards, but allows for enforcement of those standards by someone other than NIST, because NIST is not a regulatory agency.

I recommend the Consumer Finance Protection Bureau (CFPB) as the enforcement agency for data brokers. Because data brokers and credit bureaus have so many similarities I think that putting the responsibility for both at CFPB makes the most sense. The CFPB has an outstanding track record and has the capability to conduct needed examinations.[28]

The FTC should continue with its rule and oversight of the security standards of data brokers that hold data subject to COPPA regulations or who hold data about children under the age of 18. Perhaps in time, this function could also end up at CFPB, but moving the authority should not be a priority.

---

[28] The CFPB examination manual. http://files.consumerfinance.gov/f/201210_cfpb_supervision-and-examination-manual-v2.pdf

The Path Forward

I understand that there is no perfect solution here. If we change existing regulators, there will be tremendous costs and confusion. Creating a new agency just for security seems a very unlikely option today. Decentralizing responsibility is not attractive either, but it my be the best choice among the choices available. In some ways, we have become prisoners of past piecemeal decisions. This is a problem in the privacy arena as well.

While it is challenging to find any solution that will be consistent with all principles, I recommend NIST security standards and CFPB enforcement as a workable alternative. The data broker sector with its high impact, high complexity, and large data flows needs to have minimum data security standards; it is worth finding the path forward to get this work done.

Thank you for inviting me today to testify. I welcome your questions.

Respectfully,

Pam Dixon
Executive Director,
World Privacy Forum