KEEPING THE INTERNET
OPEN • INNOVATIVE • FREE

www.cdt.org

CENTER FOR DEMOCRACY
& TECHNOLOGY

1634 I Street, NW
Suite 1100
Washington, DC 20006

P +1-202-637-9800
F +1-202-637-0968
E info@cdt.org

Statement of **Justin Brookman**
Director, Consumer Privacy
Center for Democracy & Technology

Before the House of Representatives
Committee on Science, Space, and Technology

CAN TECHNOLOGY PROTECT AMERICANS FROM INTERNATIONAL CYBERCRIMINALS?

March 4, 2014

On behalf of the Center for Democracy & Technology (CDT), I thank you for the opportunity to testify today. CDT welcomes the attention the Committee has given to the pressing issues of consumer data privacy and security, especially in the context of the recent high-profile breaches that have affected a range of businesses and educational institutions.

CDT is a non-profit, public interest organization dedicated to preserving and promoting openness, innovation, and freedom on the Internet. I currently serve as the Director of CDT's Consumer Privacy Project. Our project focuses on issues surrounding consumer data, and I have previously testified before Congress on the issues of data breach, privacy, and security.

CDT's testimony today will briefly describe the impact on businesses and consumers of data breach and malicious access. I will then describe the existing legal framework covering data security, including the recently released federal cybersecurity guidelines. I will conclude with thoughts on suggested reforms – both legal and technical – that would more effectively protect consumer privacy and security. Ultimately, Congress can best protect consumer information by strengthening legal incentives for companies to better safeguard data, and by enacting comprehensive data privacy legislation to give users more insight and control over how their information is collected and used.

I. The Expanding Cost to the Economy of Data Breach

As recent events have demonstrated, data breaches can be quite broad in scope. Target reported that its 2013 data breach could have affected up to 110 million customers.[1] Neiman Marcus reported in January 2014 that unauthorized hackers had breached its servers, accessing the payment information of its own

[1] Jia Lynn Yang & Amrita Jayakumar, *Target Says Up to 70 Million More Customers were Hit by December Data Breach*, WASH. POST (Jan. 10, 2014), *available at* http://www.washingtonpost.com/business/economy/target-says-70-million-customers-were-hit-by-dec-data-breach-more-than-first-reported/2014/01/10/0ada1026-79fe-11e3-8963-b4b654bcc9b2_story.html.

customer base.[2] That same month, Michael's disclosed that its systems holding customer data may had been breached.[3] And just last month, the University of Maryland suffered a security attack affecting records containing personally identifiable information (including names, dates of birth, and Social Security Numbers) of faculty, staff, and students dating back to 1998.[4] Unfortunately, data breaches are not a new problem. In May 2011, I testified in the House Energy and Commerce Committee on the data breach issue following two high profile breaches that affected Sony Corp. and Epsilon, a major email marketing firm.[5] Those breaches, combined, affected a total of over 160 million accounts.[6] According to the Privacy Rights Clearinghouse, over 660 million records have been breached in approximately 4200 incidents since 2005.[7]

Data breaches impose substantial financial costs on businesses and consumers and also undermine consumer confidence. According to a 2013 Ponemon Institute Study, the average cost that a U.S. company incurs as a result of a data breach is $5.4 million per incident.[8] That does not count the cost to consumers. Consumers whose personal information is lost or stolen in data breaches face increased risks of identity theft, spam and phishing attacks, and sometimes humiliating loss of privacy over sensitive medical conditions. They also lose trust in the services on which they depend, which hurts both the consumers and those businesses.

There are few options for consumers who seek to avoid breaches (other than using cash for all transactions, which is not very feasible). After a breach is reported, it is often not clear what consumers can do to mitigate the consequences, especially as data breach notifications can be difficult to parse. The typical remedy – free credit reporting monitoring for a year or more – is focused on fixing a problem after it occurs rather than prospectively defending against unauthorized use of consumer data.

---

[2] Hayley Tsukayama, *Neiman Marcus Confirms Data Breach, Some Customers at Risk*, WASH. POST (Jan. 11, 2014), *available at* http://www.washingtonpost.com/business/technology/neiman-marcus-confirms-data-breach-offers-few-details/2014/01/11/56c6dc7e-7ae1-11e3-af7f-13bf0e9965f6_story.html.

[3] Hayley Tsukayama, *Michaels Discloses Possible Customer Data Breach; Secret Service Investigating*, WASH. POST (Jan. 27, 2014), *available at* http://www.washingtonpost.com/business/technology/michaels-discloses-possible-customer-data-breach-secret-service-investigating/2014/01/27/73a8538e-877c-11e3-a5bd-844629433ba3_story.html.

[4] Patrick Svitek, *University of Maryland Offers Four More Years of Credit Monitoring for Security Breach Victims*, WASH. POST (Jan. 27, 2014), *available at* http://www.washingtonpost.com/local/university-of-maryland-offers-4-more-years-of-credit-monitoring-for-security-breach-vicitms/2014/02/25/16e65e9a-9e72-11e3-a050-dc3322a94fa7_story.html.

[5] Testimony of Justin Brookman, Center for Democracy & Technology, United States House of Representatives Committee of Energy and Commerce, Subcommittee on Commerce, Manufacturing, and Trade (May 4, 2011), *available at* https://www.cdt.org/files/pdfs/20110504_bonomack_jb.pdf.

[6] Ian Sherr, Hackers Breach Second Sony Service, WALL ST. J. (May 2, 2011), *available at* http://online.wsj.com/article/SB10001424052748704436004576299491191920416.html?mod=e2tw; Les Luchter, Epsilon Confronts Possible $225M In Data Breach, MediaPost News (April 29, 2011), http://www.mediapost.com/publications/?fa=Articles.showArticle&art_aid=149603.

[7] Privacy Rights Clearinghouse, Chronology of Data Breaches, last updated February 27, 2014, http://www.privacyrights.org/data-breach/new.

[8] Ponemon Institute, "2013 Cost of Data Breach Study: Global Analysis" (May 2013), *available at* https://www4.symantec.com/mktginfo/whitepaper/053013_GL_NA_WP_Ponemon-2013-Cost-of-a-Data-Breach-Report_daiNA_cta72382.pdf.

II. More Companies, Collecting More Data

Companies also face difficulties in mitigating or avoiding the risk of security breaches. As more companies collect information in ever increasing ways through online commerce, mobile applications, and wearable devices, an increasing number of businesses are creating databases containing personal data. This means that more companies than ever before are tempting targets for hackers seeking to gain access to personal data; those companies that have not historically been prime targets for data breach may not be prepared for unauthorized third party access or its consequences. The interaction between hackers and businesses can at times resemble an arms race, with each side seeking to increase its capabilities to conduct or resist a breach.

As more businesses collect consumer data – whether through mobile applications, networked devices in the home, or ecommerce sites – data security has become an increasingly important issue for many companies that may have had little to no prior experience with creating security programs. Moreover, some companies may share data they collect with third parties, requiring reasonable security standards for the transmission of data outside of the company. As some companies may not yet have developed security programs that can withstand attacks by outsiders seeking to gain unauthorized access, the risk of data breach remains high.

One factor driving the increased collection of consumer data is the promise of "Big Data." Big data refers to datasets whose size is beyond the ability of traditional software tools to capture, store, manage, and analyze.[9] The big data trend includes not only the ongoing, exponential expansion of data collection, but also advances in computing power, storage, and the ability to analyze separate datasets. The spread of these developments has been rapid and broad.[10]

While big data holds a great deal of promise, it also requires strong security measures. As CDT has argued, any collection of personal data by companies implicates individual privacy interests.[11] Collection and retention by themselves open up companies to potential hazards – and not just from data breaches. The risk of unauthorized access by company employees, changes in company practices, and illegitimate government access all implicate individual privacy interests.

Given the widening scope of commercial data collection and the growing scale and frequency of data breaches, it is appropriate to question whether enough is being done to solve the problem. Although state and federal laws require companies to notify affected consumers of a data breach, the financial and reputational costs of notification may not provide some companies with adequate incentive to properly protect consumers' data. The goal of federal policy should be to

---

[9] James Manyika et al., *Big Data: The Next Frontier for Innovation, Competition, and Productivity,* McKinsey Global (May 2011), http://www.mckinsey.com/Insights/MGI/Research/Technology_and_Innovation/Big_data_The_next_frontier_for_innovation.

[10] For example, in 2012, Microsoft announced that Excel, part of the basic Office suite of software and a program used by many millions, will include big data analytic capabilities. *Microsoft Seeks an Edge in Analyzing Big Data,* N.Y. TIMES (Oct. 29, 2012), at B2, *available at* http://www.nytimes.com/2012/10/30/technology/microsoft-renews-relevance-with-machine-learning-technology.html.

[11] Justin Brookman & G.S. Hans, *Why Collection Matters: Surveillance as a De Facto Privacy Harm,* Future of Privacy Forum Big Data & Privacy Workshop Paper Collection (2013), *available at* http://www.futureofprivacy.org/wp-content/uploads/Brookman-Why-Collection-Matters.pdf.

incentivize both companies and government bodies to install sufficient front-end data security measures, to minimize their holdings of consumer data that is no longer necessary for a specific, legitimate purpose, and to develop structures that monitor and control where consumer data resides, without impeding innovation. Cybersecurity policy should promote substantive protections, but avoid prescribing specific technical requirements. Finally, although data breach is an important problem, new rules on data security would be best addressed as part of comprehensive baseline consumer privacy legislation.

III. The Existing Legal Framework for Security and Data Breach Notification

At the federal level, there are several sectoral laws and regulations requiring entities holding personal information to adopt reasonable security measures and, sometimes, notification to the victims of data breach. The federal laws are something of a patchwork insofar as they cover some data in certain contexts, but not others, reflecting the sector-by-sector approach Congress has thus far taken with regard to privacy rules. For example, the Federal Information Security Management Act (FISMA),[12] the Privacy Act,[13] and the Veterans Affairs Information Security Act[14] apply to the federal sector, but not the private sector. The Fair Credit Reporting Act (FCRA) applies to consumer reporting agencies,[15] the Gramm-Leach Bliley Act (GLBA) applies to covered financial institutions,[16] and the Health Insurance Portability and Accountability Act (HIPAA) and Health Information Technology for Economic and Clinical Health Act (HITECH) apply to covered health care entities.[17] Consumer data that is not covered under these laws is generally protected under the Federal Trade Commission (FTC) Act.[18]

Section 5 of the FTC Act prohibits deceptive and unfair practices in interstate commerce.[19] Although the FTC Act does not provide for notification to consumers in the event of a data breach, the FTC has used its unfairness authority to bring suits against companies for failing to adopt reasonable security procedures. Since 2004, the FTC has settled dozens of data security cases against companies that it alleged had failed to provide reasonable and appropriate protections for consumers' information.[20] The settlements have included cases involving traditional data security in the context of records containing personally identifiable information,[21] to newer technologies such as Internet-enabled video cameras that allowed consumers to monitor their homes remotely allowed unauthorized users to tap into the camera feeds.[22]

---

[12] 44 U.S.C. 3541 et seq.

[13] 5 U.S.C. 552a et seq

[14] 38 U.S.C. 5722 et seq.

[15] 15 U.S.C. 1681 et seq.

[16] 15 U.S.C. 6801 et seq.

[17] 42 U.S.C. 1320d et seq.

[18] 15 U.S.C. 45(a) et seq.

[19] *Id.*

[20] Commission Statement Marking the FTC's 50th Data Security Settlement, Jan. 31, 2014, *available at* http://www.ftc.gov/system/files/documents/cases/140131gmrstatement.pdf.

[21] *GMR Transcription Servs., Inc.*, Matter No. 112-3120 (F.T.C. Dec. 16, 2013) (proposed consent order), *available at* http://www.ftc.gov/news-events/press-releases/2014/01/provider-medical-transcript-services-settles-ftc-charges-it.

[22] *TRENDnet, Inc.*, No. 122-3090 (Sept. 4, 2013), *available at* http://www.ftc.gov/opa/2013/09/trendnet.shtm.

The FTC's ability to use its Section 5 authority to require reasonable security practices is currently being litigated in the U.S. District Court in New Jersey. The case, *FTC v. Wyndham*, concerns the security practices of the Wyndham hotel chain, which suffered three security breaches between 2008 and 2010.[23] The FTC filed a complaint against Wyndham in 2012 alleging that the company's security practices — including failing to encrypt payment data and the use of default logins and passwords — constituted unfair and deceptive practices under the FTC Act. However, rather than settling as most defendants do, Wyndham took the somewhat unusual step of challenging the FTC's case, and has moved to dismiss the case. The thrust of Wyndham's argument is that the FTC Act does not explicitly cover data security practices, and that the many subsequent bills introduced in Congress that would grant the FTC explicit, specific authority to regulate data security practices implicitly indicate that Congress did not intend to grant such authority under the FTC Act. CDT disagrees with Wyndham's argument on multiple grounds.[24] The continued recurrence of data breaches demonstrates the importance of the FTC's ability to regulate data security by bringing enforcement actions against companies with subpar security practices.

As of early 2014, 46 states, the District of Columbia, Guam, Puerto Rico, and the U.S. Virgin Islands have enacted legislation on the breach of personal information.[25] There are also several federal laws requiring notification to consumers in the event of a data breach. Although the state standards vary and the federal laws are incomplete in their coverage, most companies already do notify affected individuals in the event of a data breach. The great majority of data breach law focuses on notifying consumers after a data breach, without providing incentives or requirements regarding data collection and retention that could help prevent data breaches from occurring in the first place.

Each of the state laws provides a general time frame in which the compromised entity must notify consumers of a breach. Often, this time frame is defined as within the most expedient time possible and without unreasonable delay. Some states – such as New York[26] and Texas[27] – levy civil or criminal penalties on compromised entities if they fail to promptly notify consumers of a breach, while other states – such as California[28] – do not. Some states – such as California,[29] but not New York or Texas – allow individuals to bring a private right of action for injuries suffered as a result of violations of the breach notification law. Many states – including California,[30] New York[31] and Texas[32] – provide for some exemption from breach notification requirements when breached private information is encrypted.

---

[23] Federal Trade Commission v. Wyndham Worldwide Corporation, et al., Docket No. Case No. 2:12-cv-01365-SPL, (June 26, 2012) (complaint), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2012/06/120626wyndamhotelscmpt.pdf.

[24] G.S. Hans, *Data Security and Your Next Hotel Stay: How the FTC Encourages Strong Security Practice*, Cen. Dem. Tech. PolicyBeta Blog (May 21, 2013), https://www.cdt.org/blogs/gs-hans/2105data-security-and-your-next-hotel-stay-how-ftc-encourages-strong-security-practice.

[25] National Conference of State Legislatures, Security Breach Notification Laws (last updated January 21, 2014), http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

[26] N.Y. Gen. Bus. Law 899-aa(d)(6).

[27] Tex. Bus. & Com. Code 521.151.

[28] Cal. Civ. Code 56.06, 1785.11.2, 1798.29, 1798.82.

[29] Cal. Civ. Code 1798.84(b).

[30] Cal. Civ. Code 1798.82(e).

IV. Federal Cybersecurity Policy

The Obama administration has given some guidance to companies to promote security against cyber attacks. In February 2014, the National Institute of Standards and Technology (NIST) released its Framework for Improving Critical Infrastructure Cybersecurity, pursuant to Executive Order 13636.[33] The framework is designed to promote security for critical infrastructure within the United States, while simultaneously taking into account business considerations and privacy and civil liberties concerns.

During the process leading up to adoption of the Framework, CDT, along with fourteen other organizations, submitted comments to NIST calling for the inclusion of privacy protections based on the Fair Information Practice Principles (FIPPs) in the final Framework.[34] The FIPPs have been used for decades to effectively and flexibly promote privacy. In the drafting process, NIST had acknowledged the importance of the FIPPs,in a proposed Appendix to the draft Framework. Some commenters, however, encouraged NIST to use process-based protections, rather than the substantive protections offered by the FIPPs.[35] In its final Framework, NIST adopted a modified process-based approach. Rather than specifying at some level of detail how FIPPs could be applied to cybersecurity measures, the Framework adopts the process-based orientation for the most part.[36] It calls on organizations to assess the privacy implications of their cybersecurity programs, to have privacy-trained personnel, and to put in place processes to ensure that cybersecurity activities are lawful.

CDT supports the use of the Framework to help companies that want to more effectively secure their data from unauthorized access. However, the Framework's process-based approach gives less guidance to companies and less protection to consumers than is needed. CDT hopes that the Framework will encourage companies to consider strong privacy and security protections, ideally based on the FIPPs, when determining how to promote cybersecurity. Effective and robust security programs to guard against unauthorized data breach are necessary in order to both protect critical infrastructure and protect consumer privacy and data security.

V. Legal and Technical Solutions

Rather than prescribing specific technologies, Congress should enact legislation to sufficiently incentivize companies to implement innovative solutions to minimize data breach. At the very

---

[31] N.Y. Gen. Bus. Law 899-aa(b).

[32] Tex. Bus. & Com. Code 521.053(a).

[33] National Institute of Standards and Technology, Framework for Improving Critical Infrastructure Cybersecurity (Feb. 12, 2014), *available at* http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf.

[34] Letter from Access et al. to Adam Sedgewick, Nat'l Institute of Standards & Tech. (Dec. 13, 2013) (on file with author), *available at* https://www.aclu.org/sites/default/files/assets/preliminary_cybersecurity_framework_comments_-_privacy_and_civil_liberties_coalition.pdf.

[35] Letter from Harriet P. Pearson, Partner, Hogan Lovells US LLP, to Adam Sedgewick, Nat'l Institute of Standards & Tech. (Dec. 5, 2013) (on file with author), *available at* http://csrc.nist.gov/cyberframework/framework_comments/20131205_harriet_pearson_hoganlovells.pdf.

[36] The framework does indicate that, "organizations may consider how, in circumstances in which such measures are appropriate, their cybersecurity program might incorporate privacy principles" such as data minimization, use limitations, transparency, individual consent, redress for adverse impacts, data quality and security, and accountability and auditing measures. *Supra* note 33, at 16.

least, Congress should specifically empower the Federal Trade Commission to continue to bring actions against companies that fail to deploy reasonable security to safeguard consumer data. That use of its Section 5 authority is currently being challenged in the previously discussed *Wyndham* litigation; an adverse decision for the FTC in that case could mean that most companies bear little to no statutory liability for poor data security practices. CDT also supports granting the FTC the ability to seek civil penalties for initial violations of the FTC Act, which it currently lacks.[37] At present, the FTC can only seek civil penalties for data security violations with regard to children's online information under COPPA or credit report information under the FCRA or when a company violates an administrative order. If the agency could seek penalties for an initial violation, it would create a more effective deterrent effect for companies and encourage the adoption of more robust security programs.

CDT also supports the FTC's call for rulemaking authority under the Administrative Procedure Act.[38] Fears about requiring companies to use specific technologies are certainly warranted; CDT has long preferred to focus on best practices and strong privacy and security standards based in large part on Fair Information Practice Principles. Such regulations should give companies some flexibility in promoting consumer privacy and security. Requiring companies to adopt reasonable security standards – such as the creation, auditing, and maintenance of a comprehensive and robust security program – rather than specific technologies, would better protect consumers without relying upon a single technology to serves as a panacea.

With stronger legal incentives in place, industry will give further attention should be given to practical measures that companies can take in order to effectively promote data security and discourage data breaches. In the wake of the Target breach, for example, there were renewed calls for the adoption in the U.S. of the "chip and PIN" standard for credit cards.[39] In the United Kingdom, for example, credit cards contain a microchip (rather than the U.S. standard magnetic stripe), and customers input a PIN in order to complete the transaction. Such solutions deserve further study to determine if they are an appropriate security solution.[40]

In general, however, security cannot be thought of as a product that an organization or firm procures and then neglects, like other aspects of business operations. Security must be a practice that focuses on "defense in depth" and must be a resonating cultural element of the organization. For example, people living in cities have over time learned to take precautions such as locking the doors to their home when they leave. This practice is based on experience of those that have been burgled and people incorporating that experience into their routine. Encrypting data at rest, separating functional networks (e.g., an enterprise network versus the

---

[37] *Id.*

[38] Testimony of Chairwoman Edith Ramirez, Federal Trade Commission, United States House of Representatives Committee of Energy and Commerce, Subcommittee on Commerce, Manufacturing, and Trade (Feb. 5, 2014), *available at* http://www.ftc.gov/system/files/documents/public_statements/prepared-statement-federal-trade-commission-protecting-consumer-information-can-data-breaches-be/140205databreaches.pdf; G.S. Hans, *Target and Neiman Marcus Testify on Data Breach – But What Reforms Will Result?*, Cen. Dem. Tech. PolicyBeta Blog (Feb. 7, 2013), https://www.cdt.org/blogs/gs-hans/0702target-and-neiman-marcus-testify-data-breach---what-reforms-will-result.

[39] Alan Yu, *Outdated Magnetic Strips: How U.S. Credit Card Security Lags*, NPR All Tech Considered (Dec. 19, 2013, 5:34 PM), http://www.npr.org/blogs/alltechconsidered/2013/12/19/255558139/outdated-magnetic-strips-how-u-s-credit-card-security-lags.

[40] Abigail Wang, *Smart Chip Cards Wouldn't Have Saved Target*, PCMag (Jan. 30, 2014, 12:27 PM), http://securitywatch.pcmag.com/internet-crime/320071-smart-chip-credit-cards-wouldn-t-have-saved-target.

operations and maintenance network for point-of-sale devices), and more adversarial policing of network internals in search of insider exploits are examples of "defense in depth" security practices that are not well incorporated into many businesses that do not regularly deal with highly sensitive data – and even those that do have a hard time with these techniques.

Another possible security measure that could be effective in limiting future data breaches is the use of disposable credit card numbers. The security company Abine, for example, has developed a product called MaskMe, which allows customers to create a one-time only credit card number tied to their actual credit card account.[41] Therefore, if unauthorized individuals obtained access to the record of a financial transaction conducted using a MaskMe credit card number, they would not be able to use the credit card number to commit a fraudulent transaction, since the MaskMe number could only be used once. Credit card vendors such as Citi are also beginning to offer similar solutions directly. While its is currently easier to deploy disposable numbers for online transactions, some mobile wallet applications for smart phones (such as Google Wallet) have evolved to offer similar functionality at brick-and-mortar stores.

We are skeptical that enacting federal data breach notification legislation by itself will be effective in curtailing future data breaches. As noted above, nearly all the states already have data breach notification requirements in place. While we are sympathetic to companies' desire for uniformity of notification requirements, it should be noted that one of the primary benefits of notification requirements is to embed strong incentives to companies to avoid the significant costs of issuing data breach notifications. Merely simplifying the rules for breach notification weakens those incentives by making breach notifications less expensive to issue. If Congress does enact federal breach notification requirements, we strongly urge that such legislation is at least as strong as the best laws in place at the state level. If a federal law were to preempt state laws and replace them with a weak notification regime, the result would be a significant step backwards for consumers and data security. Moreover, federal preemption provisions should explicitly exclude general application consumer protection laws, and should only preempt state laws that govern the data elements covered by the federal statute. States should be free to enact protections for data not covered by federal law. For further recommendations on how to craft federal data breach notification legislation, please refer to the detailed proposals contained in our testimony before the Energy and Commerce Committee in 2011.[42]

VI. Future Data Breach and Security Proposals Should Be Part of Baseline Privacy Legislation

Expanding the FTC's security authority would be most effective upon passage of comprehensive federal privacy legislation. Unlike other developed countries, the U.S. currently lacks a comprehensive privacy law that would protect consumers across all sectors of the economy. The current patchwork of state laws does not provide the most effective protection for consumers. A baseline data privacy law would require companies to collect only as much personal information as necessary, be clear about with whom they're sharing information, and expunge information after it is no longer needed.

---

[41] Adam Tanner, *Why You Should Use a Masked Credit Card to Shop Online*, Forbes (Dec. 4, 2013, 12:12 PM), http://www.forbes.com/sites/adamtanner/2013/12/04/why-you-should-use-a-masked-credit-card-to-shop-online/.

[42] Testimony of Justin Brookman, Center for Democracy & Technology, United States House of Representatives Committee of Energy and Commerce, Subcommittee on Commerce, Manufacturing, and Trade (May 4, 2011), *available at* https://www.cdt.org/files/pdfs/20110504_bonomack_jb.pdf.

The Fair Information Practice Principles (FIPPs) must be the foundation of any comprehensive privacy framework. FIPPs have been embodied to varying degrees in the Privacy Act, Fair Credit Reporting Act, and other sectoral federal privacy laws that govern commercial uses of information online and offline. The formulation of the FIPPs by the Department of Homeland Security[43] and the more recent formulation adopted by the Administration in its Consumer Privacy Bill of Rights[44] offer a robust set of modernized principles that should serve as the foundation for any discussion of consumer privacy legislation. Those principles are:

- Transparency
- Purpose Specification
- Use Limitation
- Data Minimization
- Data Accuracy
- Individual Participation
- Security
- Accountability

Although data security, individual access to personal information, and notification of breaches are important safeguards under the FIPPs, it is crucial that baseline consumer privacy legislation not give short thrift to the other FIPPs, such as data minimization. Companies should collect only that data which is directly relevant and necessary to accomplish a specified purpose, and data should only be retained for as long as is necessary to fulfill a specified purpose. Unlike breach notification, data minimization is a pre-breach remedy and should be an obligation of all companies that collect personal information. Requiring companies to delete unneeded consumer data would reduce the impact of data breaches, and potentially result in fewer targets for identity thieves. We believe that requiring reasonable data minimization would result in less consumer information being exposed through data security breaches.

Comprehensive privacy legislation should also provide consumers with reasonable access to the information that companies possess about them. When companies collect, maintain, and transfer personal data to third parties, enabling individual consumers to access their personal data files and point out possible errors can provide an important safeguard against inaccuracy and misuse, and also provide needed transparency to consumers about the wide range of entities that possess and use information about them.

As data flows have grown more complex, companies must have safeguards in place to monitor them. The fact that major data breaches continue to occur demonstrates that current practices

---

[43] U.S. Department of Homeland Security, Privacy Policy Guidance Memorandum, The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security, December 2008, http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf.

[44] WHITE HOUSE, CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY (2012), *available at* http://www.whitehouse.gov/sites/default/files/privacy- final.pdf.

for collecting and storing consumer data have outstripped the practices for keeping it safe. The most effective solution will not lie in an isolated effort to apply encryption to data or to quickly notify consumers of a data breach, although both encryption and notification are important. Rather, the law should provide companies with a range of incentives and requirements that encourage them to establish internal policies that seamlessly protect data throughout the data's lifecycle. A comprehensive data protection framework coupled with strong enforcement is that solution. CDT looks forward to working with both chambers to enact strong privacy protections for American consumers.

VII. Conclusion

CDT would like to thank the Committee for calling this hearing on such an important topic, and for the opportunity to testify today.

For more information, contact Justin Brookman, justin@cdt.org, at (202) 637-9800.