Data Privacy Principles for Spurring Innovation

BY DANIEL CASTRO | JUNE 2010

Policymakers should take a balanced approach to privacy that considers both the needs of individuals and the impact on society, rather than focusing exclusively on the demands of individuals at the expense of the collective good.

Technological innovation, particularly in information technology (IT), is at the heart of America's growing economic prosperity. Crafting effective policies that boost innovation and encourage the widespread "digitization" of the economy is critical to ensuring robust economic growth and a higher standard of living. Perhaps the biggest barrier to more rapid progress toward a digitally enabled society is the fear by some people that this will entail a loss of privacy. Although IT is leading to vastly increased convenience, choice, and empowerment for individuals, some advocates see an IT-enabled world as a dystopia where our actions will be tracked by corporate or government leviathans. In this view, IT is stripping us of our privacy and exposing our intimate lives to anyone who wants to see them. As such, they argue that it is up to government not only to severely limit data collection and flows, but also to limit the very technology itself.[1]

Privacy concerns associated with IT must be taken seriously, but it is important to keep a sense of perspective. Historically, major new technologies have prompted what in hindsight were overblown privacy fears. To cite an example, some people objected to easy-to-use cameras, fearing that individuals' activities would no longer be "private' when walking down the street.[2] Or to cite another example, when transistors were first developed, there was a short-lived privacy scare that everyone would be able to be snooped on using small electronic "bugs." In fact, *Life Magazine* had a headline on it "Insidious Invasions of Privacy" and Congress even went so far as to hold hearings on the matter.[3] Of course, all this fuss was much ado about very little.

Society has always learned to manage the so-called threats in large part because of the fact that many—but certainly not all—of the concerns raised by privacy activists are hypothetical and speculative.[4] Given the large amount of information in digital format today, it is worth asking how much harm has

been done to date. Notwithstanding all the fear and gloom from privacy activists, there simply have not been widespread privacy violations caused by existing privacy laws and regulations. Moreover, the debate on privacy to date has been driven largely by privacy fundamentalists (i.e., those individuals who value personal privacy above all other values) that advocate protecting individual privacy above all else, no matter the costs or consequences. However, as with most issues, policymakers should take a balanced approach that considers both the needs of individuals and the impact on society, rather than focusing exclusively on the demands of individuals that come at the expense of the collective good.

Considered in this light, the answer to many technology-related privacy risks is not to ban IT applications entirely or to enact stringent regulations that limits beneficial uses of data, as some privacy advocates propose, but rather to ensure that the appropriate rules and practices governing privacy and civil liberties are in place and enforced. With this in mind, ITIF recommends that policymakers adhere to the following principles when crafting government regulations on data handling and use:

- Reduce roadblocks that impair the flow of data
- Foster consumer choice
- Protect individuals from harm (rather than try in vain to lock up all potentially harmful data)
- Implement strong protections for civil liberties

REDUCE ROADBLOCKS THAT IMPAIR THE FLOW OF DATA

Countless examples abound of how sharing information provides many useful benefits to individuals and society from more informed consumers to a more politically engaged society. The private sector continues to find innovative ways to unlock the hidden value of data to create value for consumers and society. Social media tools in particular are an important example of useful data sharing. Consumers have enthusiastically embraced online tools for sharing information with social networking websites like Facebook reporting over 400 million active users worldwide. Political leaders use social networking tools to communicate directly with the public. For example, President Barack Obama has over 8.6 million fans on Facebook and former Governor Sarah Palin has over 1.6 million fans.[5] Consumers share photos on websites like Flickr, videos on sites like YouTube, and opinions and reviews on sites like Yelp. The Wikimedia Foundation hosts various information sharing projects such as Wikipedia, a user-created online encyclopedia, and Wikiversity, an online community for sharing free learning resources. Overall data sharing has created a more useful and interesting experience for Internet users.

Unfortunately, many privacy activists do not just want to set the privacy rules just for themselves, they want to set them for everyone else. Evidence of this can be seen in the recent debate about the privacy settings for Facebook where privacy fundamentalists did not just simply opt not to use the service, instead they advocated for laws to impose their standard of privacy on all users. For example, Danah Boyd a fellow at Harvard's Berkman Center for Internet and Society, claimed that Facebook is a utility and should be regulated like one.[6] Others, such as Chris Conley at the American Civil Liberties Union (ACLU) stated "People are not necessarily thinking about how long this information will stick around, or how it could be used and exploited by marketer."[7] This type of paternalistic view of Internet users is at the heart of arguments in favor of government regulation to protect consumers from themselves.

Such paternalism might be justified if it did not come with significant costs. Many of these proposed regulations either limit useful types of data sharing or impose unnecessary costs on consumers.[8] For example, restriction on sharing information with third parties would limit the ability of organizations to integrate their services with other providers. Organizations would find it more difficult to partner with outside entities to create a combined service. Mash-ups—remixing data across multiple external service providers—are one of the hallmarks of the Web 2.0. For example, Microsoft Hohm allows users to monitor, compare and share their home's energy usage. Google offers an application programming interface (API) which allows developers to create their own custom map. This has resulted in many interesting mash-ups. USA Today has used the API to map all of the home foreclosures in Denver since 2006, while websites such as WikiCrimes

provide mash-ups of user-submitted crime reports, and Virginia Tech's eCorridors application constructs maps of broadband coverage and speeds from user-submitted data. The more significant risk for most consumers is not a loss of privacy, but the loss of free Internet content and services as a result of overly restrictive privacy regulations.

Policymakers should recognize that consumer privacy should not come at the expense of beneficial uses of individual data. Both for-profit and non-profit organizations collect, share and use individual data routinely to provide important services. Organizations routinely purchase contact lists from companies like Hoover's to find sales prospects and media contacts. Websites like Trulia and Zillow use public databases to collect and share home prices and property tax information. Non-profits and politicians routinely purchase data for outreach and fundraising. Organizations promoting government openness use personal data to provide online tools to foster transparency and public accountability. For example, websites like OpenSecrets.org track money in politics and the website LegiStorm provides salary information on Congressional staffers. And of course many organizations have begun to use personal data for targeted advertising. Federal data privacy legislation should ensure that beneficial uses of data are not curtailed by overly-restrictive data sharing policies.

Another significant impediment to the free flow of data is privacy regulations that create unnecessary costs for the private sector which will be borne by consumers. Proposals for expanding privacy regulations rarely consider the impact such proposals have on consumers as a group. Rather, the focus is all about the individual. Policymakers should recognize that privacy, as with any other value, must be balanced against other competing interests and can come at a real financial cost which hurts all consumers.

Examples of the impact of privacy regulations can be seen in health care.[9] The United States has made a commitment to using information technology to improve health care. In implementing health IT systems, nations must grapple with issues related to ensuring the privacy of patients' sensitive health and other personal information. If privacy laws at the state or federal level are too restrictive, they can impede the adoption of health IT and its use in clinical care. At the federal level, for example, the HIPAA Privacy Rule (45 CFR Parts 160 and 164), which provides the federal floor of privacy protection for health information in the United States while allowing more stringent state laws to continue in force, states that health care providers must "protect against any reasonably anticipated threats." This condition created much initial confusion for providers, who struggled to determine if the use of technology such as e-mail to communicate with a patient violated these terms (it does not).[10] Similarly, at the state level, a recent study of health IT adoption rates found that states with more restrictive privacy laws were less likely to have high rates of EHR usage.[11] Thus, a balance is needed in the United States that can both reassure patients that their privacy is being protected while not implementing restrictive measures that reduce data sharing and result in lower quality care.

The cost of complying with privacy regulations is one reason that any federal privacy regulations should include a preemption clause so that federal law would supersede any state regulations. To be effective, a federal framework for consumer data privacy should establish a single, nationwide standard for consumer privacy thereby reducing regulatory complexity for the private sector. If Congress does move forward with privacy legislation, it should ensure that any new regulations preempt state laws, otherwise online service providers will find themselves facing competing, and possibly contradictory, data use and handling requirements for consumers.

Health care also provides an example of how lack of government action can impede data sharing. As health IT is more widely adopted, the amount of health data that will be available to medical researchers will be increasing substantially. While past medical researchers had only a few limited data points recorded on paper on which to base their hypotheses, in the future researchers will have massive online databases containing terabytes of data for their analysis. Some of the major benefits from modernizing our health care system are expected to come from the improvements in medical research that it will enable. For example, medical researchers will be able to use rapid-learning health networks to determine the effectiveness of a particular treatment for a certain population or to discover harmful side-effects of a drug.[12] Unfortunately, the United States currently lacks the capability to share medical data for authorized research in a timely and efficient manner.[13] To address this problem, future efforts in the

United States to speed adoption of electronic health records systems should include functional requirements to allow the secondary-use of medical data for research. The goal should be to develop a national data-sharing infrastructure to support health informatics research, rather than to create isolated, project-specific research databases.

FOSTER CONSUMER CHOICE

Societal values change over time and privacy is no different. Over the course of human history, privacy itself is a relatively new value, and varies from culture to culture (and person to person). Certainly the last decade has seen a sharp rise in individuals willing to share what was previously considered private information publicly on the Internet. For example, the website NetworthIQ allows individuals to share their personal financial information online and the microblogging website Twitter allow individuals to easily share personal information, including their location, publicly and in real-time.

In response to consumer demand, the private sector has created a variety of online services catering to consumers with different types of privacy wants. Currently, websites operate under a notice and choice regime, whereby consumers can review the privacy policies, if any, offered by an organization, and then decide whether to use the services offered. For example, if a new mobile application or online service does not provide a privacy notice on their website or states that the organization will share personal information with third-parties, consumers can decide that this does not meet their standards and not use the application or service. This allows for a broad array of consumer choice between services offering different levels of privacy.

Freedom of choice to reveal or conceal private information has led to many important innovations that benefit consumers. Many, if not most, individuals routinely choose to make a trade-off of private data in exchange for something of value. In grocery stores and retail stores, consumers use loyalty cards to allow merchants to track their purchases in exchange for discounts. The same is true online—users allow websites to provide them with free or discounted content or services in exchange for targeted advertising based on personal information. This business innovation has generated an entirely new class of ad-supported online businesses. Moreover, targeted ads—advertisements relevant to a particular user—generate more than two times the revenue of non-targeted ads and are, and will continue to be, an important source of revenue for the Internet ecosystem, particularly the so-called "long tail" of small websites supported by ad revenue.[14] In addition, policymakers concerned with the decline of print media should note that greater revenue from targeted online advertising will likely be necessary for journalism to survive in the Internet age.

Individuals who place a high value on their privacy also help drive innovation. Competition between service providers, whether it is for social networking or for medical data, encourages companies to provide users with simple and effective privacy controls and ensure high levels of security to protect data.[15] Competition also encourages the development of privacy-enhancing technologies (PETs). For example, in response to consumers concerns (mostly unfounded) about the ability of advertisers to track users across multiple websites through the use of cookies (small data files stored on a user's computer by a web browser to improve the web user's experience), every major web browser now includes many features to allow users control over their online privacy and the use of cookies. Other PETs, such as anonymous Internet proxies or anonymous peer-to-peer (P2P) clients, that allow individuals to use the Internet without directly revealing their IP address, similarly have come about because of user interest.

Market forces are an important mechanism for protecting user privacy. One of the most effective ways to ensure that consumers can continue to find online services that satisfy their privacy requirements is to encourage a competitive market that responds to consumer demand. For example, although Facebook is routinely criticized by privacy activists, the company has a long history of responding to consumer pressure including in May 2010 when it announced plans to roll out new privacy controls to users in response to consumer feedback.[16] Neither was this the first time that Facebook revised its policies or services in response to consumer opinion. In December 2009, Facebook altered its privacy settings so that certain information including friends list, gender, city, and profile photo, would be public information. In response to complaints from some users, Facebook modified its

interface to give users more control over the privacy of different types of information. Similarly, in 2006, Facebook revamped its policy regarding its "news feed" feature that updates users about their friends' activities after receiving negative user feedback.

Encouraging competition that gives consumer choices between service providers is more useful than government privacy regulations that try to impose a one-size-fits-all approach to privacy.

PROTECT INDIVIDUALS FROM HARM (RATHER THAN TRY IN VAIN TO LOCK UP ALL POTENTIALLY HARMFUL DATA)

One key goal of government information policy should be to protect individuals from harm. Many tools, even if they provide important benefits, can be misused and consumers should be protected from misuse. Privacy activists often argue that government should concern itself with the mechanics of how the private sectors handles or uses data rather than the outcomes. However, additional privacy regulations cannot guarantee privacy or prevent accidental disclosures or data theft. Instead, protections should be in place to minimize or eliminate harm to consumers if private data becomes public.

Protecting individuals from harm is important because the impact of private data becoming public is more important for consumers than the mechanism by which it becomes public. For example, individuals concerned about employment discrimination because of their health conditions are better served by strong anti-discrimination regulations that prevent harmful uses of private data than by arbitrary restrictions and limitations on legitimate uses of this data. Often, consumers are already protected from the hypothetical harms envisioned by privacy activists by existing regulations. For example, privacy advocates recently expressed concern that lenders might deny loan applications based on information found on social networking websites even though these lenders would be in violation of the Fair Credit Reporting Act.[17] Similarly privacy concern are sometimes raised for health IT applications involving data sharing. These issues become even more complicated when data must flow internationally, such as when a health care worker is located in another country. For example, teleradiology can involve sharing personal medical data with health care workers not directly involved in a patient's care. However, such concerns are probably unnecessary as patients can hold the original source of the data (i.e. their health care provider) accountable for misuse of their data.

Protecting individuals from harm is important because the impact of private data becoming public is more important for consumers than the mechanism by which it becomes public.

Emphasizing the need for government to protect users from harm does not mean organizations are given a free pass to use consumer data without any restrictions. Importantly, organizations must adhere to their stated privacy policies. Protecting users from harm involves enforcing existing regulations. The Federal Trade Commission (FTC), for example, already has sufficient authority to protect consumers from unfair or deceptive trade practices. This means that companies, for example, cannot pull a "bait and switch" on consumers where they promise not to use data in a certain manner and then do so. Where possible, policymakers should first try to improve enforcement of existing policies rather than adding yet another layer of complexity to the existing patchwork of federal laws regulating consumer privacy, including the Gramm-Leach-Bliley Act, the Fair Credit Reporting Act, the Health Insurance Portability and Accountability Act and the Fair Debt Collection Practices Act. Additional legislation would likely end up imposing more costs on consumers and limiting innovation and the development of new online services. Policymakers should recognize that privacy, as with any other value, must be balanced against other competing interests and can, as it will here, come at a real financial cost.

IMPLEMENT STRONG PROTECTIONS FOR CIVIL LIBERTIES

To be sure, as more and more information is created in a digital format, the ease of aggregating information and tying it to individuals has grown. However, in most nations, a series of rules and laws govern how government actors can use personal data, electronic or otherwise. In fact, many of the privacy fears are not about technology, but rather about government access to sensitive information. The fact that more information is in digital form does not change this in any way.

These questions routinely appear as new technologies are introduced that use private information from cloud computing to e-books to the smart grid. For example, the prospect of vehicle manufacturers installing dedicated short-range communication (DSRC) tags on every car, begs the thorny question of who will have access to the tags, what they can do with the information, and whether access will require consent from the driver or vehicle owner. Will government be able to use this information to police violations of speed limits, red lights, and stop signs? Will police have access to vehicle travel histories or real time access to vehicle locations for use in criminal investigations? These are important questions that must be addressed with new technology. Improper use of consumer data by government is a legitimate threat that might prevent more widespread use of technologies like cloud computing. As ITIF and others have argued previously, Congress should act to reform laws such as the Electronic Communications Privacy Act (ECPA) to ensure that citizens have a right to privacy for their electronic data whether it is stored at home on a PC or remotely in the cloud.[18]

Similarly, civil liberties groups have objected to many applications of data mining because of privacy concerns stemming from the risk of data misuse. Some of their concerns arise from the fact that the government's data-mining projects involve data collected from both the public and private sectors. An additional concern is that the proliferation of digital information will lead to privacy violations by the government. The suspension of the U.S. government's Total Information Awareness (TIA) data-mining initiative—eventually renamed the Terrorism Information Awareness Program—reflects the degree of privacy advocates' concern with government data-mining programs. The TIA program established by the Defense Advanced Research Projects Agency was discontinued early in the project's lifecycle, so the privacy concerns raised by civil liberties groups were primarily about potential risks rather than actual problems.[19]

Although data mining does not provide investigators a crystal ball, it still can provide insights and clues into investigations. And the benefits of data-mining programs have not yet been fully explored. As data-mining techniques improve, with better data sources, refined algorithms, and lower false-positive rates, societies must continue to find the appropriate balance between privacy and security. But government should not let legitimate uses of technology to improve public safety get sidelined because of potential abuses; instead it should find ways to use technology effectively while ensuring that civil liberties are protected (as it should be noted, the design of TIA was intended to do).

CONCLUSION

As data on individuals or their actions increasingly is collected and stored electronically, it is important for policymakers to consider the effect this has on privacy. This Notice of Inquiry provides a welcome opportunity to explore the best ways of protecting individual privacy while avoiding constraints on business innovation and unintended negative impacts on consumers as a whole. Privacy is important, but it must be balanced against competing goals including usability, cost and future innovation. While many technologies can be misused, they should not be banned simply because they come with some risk. Privacy fundamentalists often overstate privacy concerns as a rationale for opposing certain innovations: we have seen this in everything from RFID to biometrics to electronic health records.[20] Moreover, restrictive privacy regulations for the private sector would likely result in less innovation, fewer free services for the average user, and higher costs for consumers. Instead, policymakers should embrace principles that support consumer privacy, but not at the expense of productivity and innovation.

ENDNOTES

1. For example, see the debate about using smart ID cards.

2. For a modern day example of misplaced privacy fears, see Daniel Castro, "I Spy a Luddite: Why the Lawsuit over Google Street View is Absurd," Information Technology and Innovation Foundation, Washington, D.C., April 25, 2008, http://www.itif.org/files/WM-2008-03.pdf.

3. John Neary, "Electronic Snooping—Insidious Invasions of Privacy," *Life Magazine,* May 20, 1966. http://www.bugsweeps.com/info/life_article.html.

4. Robert D. Atkinson, "RFID: There's Nothing to Fear Except Fear Itself," remarks at the 16th Annual Computer, Freedom and Privacy Conference, Washington, D.C., May 4, 2006, http://www.itif.org/files/rfid.pdf.

5. As of June 7, 2010. Source: Facebook.com.

6. Dana Boyd, "Facebook is a utility; utilities get regulated," May 15, 2010, http://www.zephoria.org/thoughts/archives/2010/05/15/facebook-is-a-utility-utilities-get-regulated.html.

7. Brad Stone, "For Web's New Wave, Sharing Details Is the Point," New York Times, April 22, 2010, http://www.nytimes.com/2010/04/23/technology/23share.html.

8. Daniel Castro, "ITIF Comments on Draft Privacy Legislation," Information Technology and Innovation Foundation, May 25, 2010, http://www.itif.org/files/2010-privacy-legislation-comments.pdf.

9. Daniel Castro, "Explaining International IT Application Leadership: Health IT," Information Technology & Innovation Foundation, September 22, 2009, http://www.itif.org/files/2009-leadership-healthit.pdf.

10. Laura Parker, "Medical-privacy law creates wide confusion," *USA Today*, October 16, 2003, http://www.usatoday.com/news/nation/2003-10-16-cover-medical-privacy_x.htm.

11. Amalia Miller and Catherine Tucker, "Privacy Protection and Technology Diffusion: The Case of Electronic Medical Records," Management Science, 55 (July 10, 2009): 1077-1093.

12. Lynn M. Etheredge, "A Rapid-Learning Health System," Health Affairs, 26 (2007): w107-w118.

13. Daniel Castro, "The Role of Information Technology in Medical Research," 2009 Atlanta Conference on Science, Technology and Innovation Policy, October 2009, http://www.itif.org/files/2009-it-medical-research.pdf.

14. "Study finds behaviorally-targeted ads more than twice as valuable, twice as effective as non-targeted online ads," Network Advertising Initiative, press release, March 24, 2010, http://www.networkadvertising.org/pdfs/NAI_Beales_Release.pdf.

15. Daniel Castro, "Improving Health Care: Why a Dose of IT May Be Just What the Doctor Ordered," Information Technology and Innovation Foundation, October 2007, http://www.itif.org/files/HealthIT.pdf.

16. Mark Zuckerberg, "Making Control Simple", Facebook.com, May 26, 2010, http://blog.facebook.com/blog.php?post=391922327130.

17. Catharine Smith, "Lenders Mine Facebook, Twitter For Info On Borrowers," June 4, 2010, http://www.huffingtonpost.com/2010/06/04/lenders-use-facebook-twit_n_600408.html.

18. "ITIF Calls for Updates to Privacy Laws," Information Technology and Innovation Foundation, March 30, 2010, press release, http://www.itif.org/pressrelease/itif-calls-updates-privacy-laws.

19. "Counterterrorism 2.0: Using IT to Connect the Dots," Information Technology and Innovation Foundation, February 23, 2010, http://www.itif.org/events/counterterrorism-20-using-it-connect-dots.

20. See Robert D. Atkinson, "RFID: There's Nothing To Fear Except Fear Itself," 16th Annual Computer, Freedom and Privacy Conference (Washington, DC: May 4, 2006), Robert D. Atkinson, "Confronting Biometric Detractors," 2006 Biometric Consortium Conference (Baltimore, MD: September 21, 2006), and Daniel Castro, "Improving Health Care: Why a Dose of IT May Be Just What the Doctor Ordered," (Washington, DC: ITIF, 2007).

ABOUT THE AUTHOR

Daniel Castro is a Senior Analyst with Information Technology and Innovation Foundation. His research interests include technology policy, security, and privacy. Mr. Castro has a B.S. from the School of Foreign Service at Georgetown University and an M.S. in information security technology and management from Carnegie Mellon University.

ABOUT THE INFORMATION TECHNOLOGY AND INNOVATION FOUNDATION

The Information Technology and Innovation Foundation (ITIF) is a Washington, DC-based think tank at the cutting edge of designing innovation policies and exploring how advances in technology will create new economic opportunities to improve the quality of life. Non-profit, and non-partisan, we offer pragmatic ideas that break free of economic philosophies born in eras long before the first punch card computer and well before the rise of modern China and pervasive globalization.

ITIF, founded in 2006, is dedicated to conceiving and promoting the new ways of thinking about technology-driven productivity, competitiveness, and globalization that the 21st century demands. Innovation goes far beyond the latest electronic gadget in your pocket – although these incredible devices are emblematic of innovation and life-changing technology. Innovation is about the development and widespread incorporation of new technologies in a wide array of activities. Innovation is also about a mindset that recognizes that information is today's most important capital and that developing new processes for capturing and sharing information are as central to the future as the steam engine and trans-Atlantic cable were for previous eras. This is an exciting time in human history. The future used to be something people had time to think about. Now it shows up every time we go online.

At ITIF, we believe innovation and information technology are at the heart of our capacity to tackle the world's biggest challenges, from climate change to health care to creating more widespread economic opportunity. We are confident innovation and information technology offer the pathway to a more prosperous and secure tomorrow for all citizens of the planet. We are committed to advancing policies that enhance our collectivecapacity to shape the future we want - beginning today.

ITIF publishes policy reports, holds forums and policy debates, advises elected officials and their staff, and is an active resource for the media. It develops new and creative policy proposals to advance innovation, analyzes existing policy issues through the lens of advancing innovation and productivity, and opposes policies that hinder digital transformation and innovation.

For more information contact ITIF at 202-449-1351 or at mail@itif.org, or go online to www.itif.org.
ITIF | 1101 K St. N.W. | Suite 610 | Washington, DC 20005