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

The Role of Privacy by Design in Protecting Consumer Privacy

Comments of the Center for Democracy & Technology In regards to the FTC Consumer Privacy Roundtable

Privacy Roundtables - Comment, Project No. P095416

December 21, 2009

The Center for Democracy & Technology (CDT) welcomes the opportunity to submit comments for the FTC's second in a series of public roundtable discussions exploring the privacy challenges posed by 21st-century technology and business practices that involve the collection and use of consumer data. CDT views these roundtable sessions as a historic opportunity to develop the record to support a new comprehensive privacy protection policy for the next decade.

As new technologies enable the collection of greater amounts of data online, it is essential that companies consider privacy at each stage of product development. Privacy by Design, a concept prominently championed by Ontario's Information and Privacy Commissioner Anne Cavoukian, presents a set of "foundational principles" to guide innovation in a manner that is consistent with Fair Information Practices (FIPs). Privacy by Design offers a roadmap to integrate privacy considerations into business models, product development cycle, and new technologies.

CDT urges the FTC to encourage business practices that are consistent with Privacy by Design by acting on the following recommendations:

- The FTC should release a set of recommendations outlining the role that Privacy by Design can play in implementing a new set of comprehensive FIPs. These recommendations should emphasize the role of privacy impact assessments, privacy threshold analyses, the integration of PETs into product development, end-to-end lifecycle protection for data, and privacy as the default or as a clear, easy-to-understand alternative.
- As location data becomes ubiquitous, the FTC should promote innovation in Privacy Enhancing Technologies and should help foster industry collaboration to ensure that location data receives the protections that such sensitive information requires.
- Through the release of rule-making or reports, the Commission should further seek to ensure that location data is being protected throughout its lifecycle and that companies and application builders alike are minimizing data collection, data use and retention, and maximizing transparency, individual participation, security, data quality, integrity, and accountability.

- The Commission should not shy away from bringing cases against bad actors that unfairly or deceptively collect location data or track consumers.
- In the behavioral advertising space, the FTC should support the development of protocols that will help enable Privacy by Design and encourage innovation that will help automate compliance.

Privacy by Design, while important, should be seen as one tool in a larger toolkit of policy approaches; it is insufficient to protect consumer privacy alone. Efforts to encourage a Privacy by Design approach to innovation should be supplemented by a rigorous mix of self-regulation, enforcement of existing law, and enactment of a new consumer privacy statute that establishes baseline protections and gives the FTC rulemaking authority.

Introduction

The Center for Democracy & Technology (CDT) is pleased to have the opportunity to submit comments to the Federal Trade Commission (FTC) to inform the second roundtable discussion exploring the privacy challenges posed by 21st-century technology and business practices.

The increasingly widespread collection, transfer and use of consumer data pose privacy risks that should be addressed as part of a comprehensive privacy agenda. As explained in the comments we submitted to the Commission in advance of the first privacy roundtable, any discussion of consumer privacy – whether in Congress, at the FTC, or within industry – must be grounded in a comprehensive set of Fair Information Practice principles (FIPs).[1] These principles include: Transparency, Individual Participation, Purpose Specification, Data Minimization, Use Limitation, Data Quality and Integrity, Security, and Accountability and Auditing.

In our earlier comments, we focused on the substantive protections that are currently lacking as consumers seek ways to assert broad control over their privacy. In this set of comments, we discuss how Privacy by Design – the incorporation of privacy into the very fabric of new technologies and the policies that govern them –– can help assure these substantive protections. We present two case studies, Location Data and Behavioral Advertising, to illustrate the privacy risks associated with and exacerbated by newly developed technologies, and we detail how Privacy by Design can be used to manage these risks.

Privacy Enhancing Technologies or Privacy by Design?

In the comments we submitted to the FTC in advance of the first privacy roundtable, we urged the Commission to promote the development of privacy enhancing technologies (PETs). PETs, such as encryption software, anonymizers, and browser extensions that provide granular data controls, promote FIPs through technology. As they have been

[1]For a more detailed discussion of the role of FIPs in comprehensive consumer privacy protection, *see* Center for Democracy & Technology, *Refocusing the FTC's Role in Privacy Protection: Comments of the Center for Democracy & Technology In regards to the FTC Consumer Privacy Roundtable* (Nov. 2009), *available at* http://www.cdt.org/files/pdfs/20091105_ftc_priv_comments.pdf ("CDT First Roundtable Comments").

traditionally understood, PETs are most useful for users who already understand online privacy risks. They are essential user empowerment tools, but they form only a single piece of a broader framework that should be considered when discussing how technology can be used in the service of protecting privacy.

Simply put, PETs, when relegated to afterthoughts and product add-ons do not fulfill the larger goal of crafting a set of consumer rights and company responsibilities that together fortify and protect the decisions that consumers make online. Data is poorly protected, for example, if a consumer's choice over whether to accept traditional tracking cookies is circumvented by the placement of flash cookies onto her computer. Moreover, once data has been collected, PETs cannot prevent secondary uses nor can they limit how the data is shared, sold, and combined with other data in the future.

Browser cookie controls provide a useful example of the limitations of PETs, and of the importance of Privacy by Design, a term coined by Ontario's Information and Privacy Commissioner Ann Cavoukian to describe a more comprehensive approach to incorporating the benefits of privacy technologies into the process of innovation. When cookies were first introduced on the Web, browsers provided no way for users to control their use.[2] As concerns were raised about potentially privacy-invasive uses of cookies, browser vendors began to add cookie controls into their products, beginning with rudimentary tools and evolving over time to the more sophisticated controls in place today.

While existing cookie controls can serve as powerful privacy protection for those who understand how to use them, for many Internet users these controls are too complicated. This is part of the reason why CDT and others have supported simpler consumer choice mechanisms.[3] If cookies and their associated browser functionality had been designed with privacy in mind from the very beginning, it is highly unlikely that cookies and the technologies available for controlling them would look the way they do today.

As described by Cavoukian, "Privacy by Design asserts that the future of privacy cannot be assured solely by compliance with regulatory frameworks; rather, privacy assurance must ideally become an organization's default mode of operation." Privacy by Design presents a set of "foundational principles" that can help companies innovate in ways that are consistent with FIPs. These seven principles are list in abbreviated form below[4]:

- **Proactive, not Reactive; Preventative, not Remedial.** The Privacy by Design approach. . .anticipates and prevents privacy invasive events before they happen. [It] does not wait for privacy risks to materialize, nor does it offer

[2] *See* Federal Trade Commission Staff Report. *Public Workshop on Consumer Privacy on the Global Information Infrastructure, Part III: Enhancing Consumer Protection Online* (Dec. 1996), *available at* http://www.ftc.gov/reports/privacy/Privacy4.shtm.

[3] *See* Center for Democracy and Technology, Consumer Action, Consumer Federation of America, Electronic Frontier Foundation, Privacy Activism, Public Information Research, Privacy Journal, Privacy Rights Clearninghouse, and World Privacy Forum, *Consumer Rights and Protections in the Behavioral Advertising Sector: Comments in Regards to The FTC Town Hall, "Ehavioral Advertising: Tracking, Targeting, and Technology"* (November 2007), *available at* http://www.cdt.org/privacy/20071031consumerprotectionsbehavioral.pdf.

[4] Anne Cavoukian, *Privacy by Design: The 7 Foundational Principles* (August, 2009)*, available at* http://www.ipc.on.ca/images/Resources/7foundationalprinciples.pdf.

remedies for resolving privacy infractions once they have occurred – it aims to prevent them from occurring.

- **Privacy as the Default.** If an individual does nothing, their privacy still remains intact.
- **Privacy Embedded into Design**. Privacy by Design…is not bolted on as an add-on, after the fact. The result is that privacy becomes an essential component of the core functionality being delivered. Privacy is integral to the system, without diminishing functionality.
- **Full Functionality – Positive-Sum, not Zero-Sum.** Privacy by Design avoids the pretense of false dichotomies, such as privacy vs. security, demonstrating that it is possible to have both.
- **End-to-End Lifecycle Protection.** Privacy by Design, having been embedded into the system prior to the first element of information being collected, extends throughout the entire lifecycle of the data involved, from start to finish.
- **Visibility and Transparency.** Privacy by Design seeks to assure all stakeholders that whatever the business practice or technology involved, it is in fact, operating according to the stated promises and objectives, subject to independent verification.
- **Respect for User Privacy.** Above all, Privacy by Design requires architects and operators to keep the interests of the individual uppermost by offering such measures as strong privacy defaults, appropriate notice, and empowering user-friendly options.

These principles represent one set of tools that can help companies realize the implementation of a comprehensive set of FIPS; they suggest how some – though not all – of the privacy concerns raised *by* new technologies can be addressed *through* new technologies and solid business practices.

Cavoukian has published a Privacy by Design Diagnostic Tool Workbook that companies can use to determine whether and how they are complying with Privacy by Design principles.[5] Meanwhile, many companies, including IBM, Sun Microsystems, Hewlett-Packard and Microsoft have already incorporated Privacy by Design into their product development processes and made strong statements about the important role that protecting privacy plays in their business models.[6]

Microsoft's implementation of its "Security Development Lifecycle" (SDL) for software development provides one example of how privacy can be built into the design process.[7]

---

[5] *See* Anne Caovukian, *Privacy Diagnostic Tool (PDT) Workbook* (August, 2001)*, Version 1.0, available at* www.ipc.on.ca/images/Resources/pdt.pdf.

[6] *See* e.g., IBM, *Privacy is Good for Business: An Interview with Chief Privacy Officer Harriet Pearson*, *available at* http://www-03.ibm.com/innovation/us/customerloyalty/harriet_pearson_interview.shtml; Microsoft Corporation, *Privacy Guidelines for Developing Software and Services* (February 2009) at 5, *available at http://www.microsoft.com/downloads/details.aspx?FamilyId=C48CF80F-6E87-48F5-83EC-A18D1AD2FC1F&displaylang=en* ("Microsoft Privacy Guidelines")*;* Hewlett-Packard Development Company, *Protecting Privacy at HP: Giving Individuals More Control over their Information* (August, 2007), *available at* http://h41111.www4.hp.com/globalcitizenship/uk/en/pdf/Privacy_casestudy_hires.pdf; Michelle Dennedy, *Sun Privacy-enhancing Desktop Technologies* (January 2009)*, Available at* http://www.privacybydesign.ca/speaker-dennedy.htm.

[7] *See* Microsoft Corporation, *Microsoft Security Development Lifecycle - Process Guidance* (2009), *available at http://msdn.microsoft.com/en-us/library/84aed186-1d75-4366-8e61-8d258746bopq.aspx* ("Microsoft SDL"). These guidelines are made available online in a form that tracks, but is abbreviated from, those used by Microsoft internally.

SDL aims to integrate privacy and security principles into the software development lifecycle, but each stage of Microsoft's 5-stage development lifecycle also includes privacy recommendations and requirements, which range from the procedural to the technical. Privacy impact ratings are given to each project and these ratings determine the design specifications needed for compliance. The SDL guidelines are supplemented by Microsoft's "Privacy Guidelines for Developing Software and Services,"[8] a document that lays out guidelines that track some of Cavoukian's Privacy by Design principles, for example End-to-End Lifecycle Protection, Privacy Embedded into Design, and Proactive, not Reactive Design. Microsoft's SDL and guidelines are not perfect.[9] But Microsoft's work in this space remains a positive example of how privacy impact can be evaluated during the planning stages of innovation, how this evaluation can be incorporated into product development, and how Privacy by Design can help ensure that FIPs such as Data Minimization, Individual Participation, and Security are heeded.

As the Commission seeks to promote implementation of a more robust set of FIPs that will benefit companies and consumers alike, we urge it to look to proactive approaches taken by companies, guidelines like Cavoukian's workbook, and documents such as CDT's Threshold Analysis, a framework developed with companies and advocates in our Internet Privacy Working Groups to help online advertisers evaluate their practices as a precursor to a full privacy impact assessment or fair information practices analysis.[10] If as we urge, the Commission releases an updated, comprehensive set of FIPs following the roundtables, we hope it will emphasize the role that Privacy by Design can play in implementing these principles. The FTC should publish best practices for Privacy Impact Assessments and third-party application vetting processes.

Below, we discuss how Privacy by Design can be used to mitigate the privacy risks associated with a location-enabled Web and behavioral advertising.

A. Privacy by Design: Location Data

The ubiquity of increasingly high-powered mobile devices has already spawned the Internet's first generation of location-based services and applications. As the accuracy of location data improves and the expense of calculating and obtaining it declines, location may well come to pervade the online experience. While the increasing availability of location information paves the way for exciting new applications and services, the increasingly easy availability of location information raises significant privacy concerns. Because individuals often carry their mobile devices with them, location data may be collected everywhere and at any time, often without user interaction, and it may

---

[8] *See* Microsoft Privacy Guidelines

[9] The guidelines, for example, do not fully implement a comprehensive set of FIPS into the design process; they rely on an outdated distinction between personally identifiable information and non-personally identifiable information that is too simplistic and should no longer be central to the privacy framework in this space*, See* Microsoft Privacy Guidelines. For a discussion about how the identifiability of data should be reconceptualized, *See* Center for Democracy and Technology, *Online Behavioral Advertising: Industry's Current Self-Regulatory Framework is Necessary, but Still Insufficient On Its Own to Protect Consumers* (December, 2009) at 10-11, *available at http://www.cdt.org/files/pdfs/CDT%20Online%20Behavioral%20Advertising%20Report.pdf* ("CDT Behavioral Advertising").

[10] Center for Democracy & Technology, *Threshold Analysis for Online Advertising Practices* 16 (Jan. 2009), *available at* http://www.cdt.org/privacy/20090128threshold.pdf.

potentially describe both what a person is doing and where he or she is doing it. Location information can also be highly identifiable: for many people, there is one location where they spend their daytime hours (at work) and one location where they spend their nighttime hours (at home). After a day or two of collecting just those two data points about a person, it becomes fairly obvious whom those data points describe.

The year 2009 saw the dawn of the location-enabled Web, as all of the major browser vendors began integrated location awareness into their browsers. For example, with the release of the iPhone 3.0 software, the latest version of the Safari web browser running on the iPhone is now location-enabled. This means that any Web site can ask Safari for the user's location, and Safari can provide it by using the location positioning technologies built into the phone (including GPS, among others). Apple has implemented a simple interface (based on a draft of a W3C standard) that Web sites can use to request location. Firefox, Opera, and Chrome are now all providing similar functionality.

The browsers provide strong baselines for consent to location sharing. On the iPhone, each Web site that wants to use location has to first obtain the user's permission not once, but twice. Those permissions are reset every 24 hours. This is a good example of "Privacy as the Default," one of Cavoukian's seven foundational principles for Privacy by Design.

But in terms of providing more granular control and transparency, the browsers are lacking. On the iPhone, there is no way for a user to see with which sites (or applications, for that matter) he or she has shared location. If a user visits a site and declines to provide location to it, the site may continue to prompt the user to provide location on every visit. It would be helpful for users to be able to have a whitelist of trusted sites that can always obtain the user's location, and a blacklist of untrusted sites that cannot ever access it.[11] That way, users could avoid the 24-hour permission renewal described above and they would not be badgered into consenting by accident.

This kind of granularity would also help with permission revocation. Right now, to revoke even a single site's permission, the only choice is to revoke all sites' permissions. Even accomplishing that is a counterintuitive process: under the general settings, using the tab marked "Reset" (a somewhat scary name), the user must select "Reset Location Warnings." Granted, the 24-hour permission relapse means that, today, there probably will not be many sites to revoke permissions from. But if the permission model ever changes, the revocation model needs to change as well.

Given the privacy interests at stake and the relative lack of protection in the law, we would expect location controls to be better than other kinds of technological controls on the Web, to offer users more choices about what happens to their data and to be especially transparent about when location data is being passed around. For example, much like the "lock" icons that indicate a secure connection, an icon could be displayed on the browser whenever Safari is transmitting location data. The FTC should promote

[11] CDT has been working for years to incorporate some of these concepts into technical standards, originally in the IETF's Geopriv working group and more recently within the W3C Geolocation working group, which created the draft standard that Apple and other browser vendors are starting to use. Incidentally, the IETF's Geopriv work has a built-in whitelisting capability, *See* http://www.ietf.org/dyn/wg/charter/geopriv-charter.html.

innovation of this type and should help foster industry collaboration to make sure that location data receives the protections that such sensitive information requires.

In the behavioral advertising context, we have urged the FTC to consider location information to be "sensitive" data worthy of heightened protections.[12] In general, location information collected for any purpose is sensitive, and we encourage the FTC to work to address the many unanswered questions about how location data is being collected, used, secured, and shared. Thus, in addition to promoting the development of PETs, the Commission should investigate, using its subpoena power if necessary, the uses of location data and whether customers are being tracked against their will. Through the investigation and reports, the Commission should further seek to ensure that location data is being protected throughout its lifecycle and that companies and application builders alike are giving sensitive location data the respect it deserves in terms of minimizing data collection and data uses and maximizing transparency, individual participation, security, data quality and integrity, and accountability. Finally, the Commission should not shy away from bringing cases against bad actors that unfairly or deceptively collect location data or track consumers.

B. Privacy by Design: Behavioral Advertising

Massive increases in data processing and storage capabilities have allowed advertisers to track, collect and aggregate information about consumers' Web browsing activities and to compile individual profiles that are used to match advertisements to consumers' interests. All of this is happening in the context of an online environment where more data is collected – and retained for longer periods – than ever before.

As CDT discussed in the comments we submitted prior to the Commission's first privacy roundtable, behavioral advertising poses significant risks to consumer privacy.[13] Data collected about users' site preferences, search terms, purchasing behaviors, and friends can be sensitive in nature, yet few data entities in the business of data collection allow users to edit or delete information associated with them, their browser, or their machine.[14] Although privacy tools are now built into all of the major browsers and trade associations are beginning to offer opt-out tools, some companies have consistently sought to circumvent user control by relying on alternative technologies.

One method for circumventing user control makes use of "Flash cookies" (also known as local shared objects), which provide storage for a persistent identifier on the user's computer. When a Flash cookie is placed on a user's computer by a company that has already placed an HTTP cookie on the user's browser, the unique ID of the HTTP cookie stored on the user's browser is associated with the Flash cookie. When the HTTP cookie

[12] *See* CDT Behavioral Advertising at 11-12,

[13] *See* CDT First Roundtable Comments.

[14] *See* CDT Behavioral Advertising at 25-28.

is deleted using browser controls, the flash cookie can "respawn" an identical HTTP cookie with the exact same ID.[15]

In August 2009, researchers at UC-Berkley reported that a number of companies were respawning cookies, including Network Advertising Initiative (NAI) member Quantcast. Quantcast, the researchers discovered, was respawning cookies on users who had opted out of targeted advertising using the NAI opt-out tool.[16] Although it appears Quantcast has since changed its practices,[17] their original disregard for consumers' choices calls into question the utility of self-regulatory guidelines and the implementation of narrowly-designed PETs like the NAI opt-out. A company that was recently admitted to the Interactive Advertising Bureau (IAB) has bragged about their use of Flash cookies to circumvent user control.[18] These practices represent unfair and deceptive acts that we encourage the FTC to investigate.

Respawning Flash cookies is but one example of the myriad methods being used to circumvent consumer control. Internet users' browser histories are increasingly being viewed as valuable, despite the obvious privacy concerns raised by the practice of mining these histories.[19] As companies have taken advantage of new technologies to develop new ways to circumvent user control, tools, practices, and regulations meant to protect consumer privacy have failed to keep up. There is no reason that this should be the case. Browser developers could have integrated flash controls into their cookie controls and protected histories by default in the releases after these problems became well known and should be encouraged to do so now.

More broadly, a commitment to Privacy by Design by trade associations and companies that play a role in the behavioral advertising eco-system would prevent deceptive practices like respawning and spying on browser histories and help build a framework of trust that might make consumers more willing to share their data for the purposes of behavioral advertising:[20] consumers who wish to avoid data collection would be able to

---

[15] *See e.g.,*Center for Deomcracy and Technology, *Applying the FTC's Spyware Principles to Behavioral Advertising: Comments of the Center for Democracy and Technology in Regards to the FTC Town Hall, "Ehavioral Advertising: Tracking, Targeting, and Technology"* (October 2007) at 3-6, *available at* http://www.cdt.org/privacy/20071019CDTcomments.pdf; Center for Democracy and Technology, Consumer Action, and Privacy Activism, *In Regard to the FTC Staff Statement, "Online Behavioral Advertising: Moving the Discussion Forward to Possible Self-Regulatory Principles"* (April 2008) at 9-12, *available at* http://www.cdt.org/privacy/20080411bt_comments.pdf; Soltani, Ashkan, Canty, Shannon, Mayo, Quentin, Thomas, Lauren and Hoofnagle, Chris Jay, Flash Cookies and Privacy (August, 2009). Available at SSRN: http://ssrn.com/abstract=1446862.

[16] Soltani, Ashkan, Canty, Shannon, Mayo, Quentin, Thomas, Lauren and Hoofnagle, Chris Jay, Flash Cookies and Privacy (August, 2009). Available at SSRN: http://ssrn.com/abstract=1446862.

[17] Ryan Singel, *Flash Cookie Researchers Spark Quantcast Change*, Wired (August 2009), *available at* http://www.wired.com/epicenter/2009/08/flash-cookie-researchers-spark-quantcast-change/

[18] *See, e.g.*, Laurie Sullivan, *Moving Flash Cookies into Direct-Response BT*, MediaPost Blogs (Sept. 16, 2009), http://www.mediapost.com/publications/?art_aid=113594&fa=Articles.showArticle (last visited Oct. 16, 2009) (describing the actions of Tatto Media).

[19] *See e.g.,* Tealium Social Media (accessed December, 2009), *available at* http://www.tealium.com/products/social-media/; *Vote! How to Detect the Social Sites your visitors use* (May, 2008), *available at* http://www.azarask.in/blog/post/socialhistoryjs/

[20] If given a choice, 68% of Americans "definitely would not" allow advertisers to follow them online even if their online activities would remain anonymous. 19% "probably" would not allow this tracking. *See* Joseph Turow, Jennifer King, Chris Jay Hoofnagle, Amy Bleakley & Michael Hennessy, *Contrary to What Marketers Say, Americans Reject Tailored Advertising and Three Activities that Enable It* (Sept. 2009), *available at*

do so and consumers who allow for collection could feel confident that information collected is transparent, limited in scope, secure, and accessible to them, not just to the companies that track them.

A commitment to Privacy by Design could yield marked improvements for privacy in the current ecosystem, one in which an extraordinary level of Internet savvy and detective work are necessary to determine which advertising networks are collecting data on any one Web site.[21] A standard that required data-collecting objects be denoted by HTTP headers, for example, would make data collection more transparent and easier to control. The code for beacons and cookies could even include information about where to find their behavioral profiles. Such a standard would enable browsers to act as a dashboard through which consumers could control the data collected about them and find the profiles being created around their data. Browsers could further implement the "privacy as a default" principle of Privacy by Design by encouraging consumers to work through a Privacy Wizard when they first install or update their browsers.

Outside of the browser, advertising networks should be encouraged to build data collection, transfer, and use architectures and best practices with privacy considerations in mind. Entities engaged in behavioral advertising should use threshold analyses and Privacy Impact Assessments to determine the level of protection that the data they are collecting requires. Privacy Impact Assessments should link the amount of data collected to the purpose for which data is being used; limitation on data use and transfer should be set in the planning stages of any product. Protocols for storing, transferring, and deleting collected data should be part of product development.

The IAB's self-regulatory guidelines include language that, although unfortunately limited to one subset of data collectors, serves as one positive example of how privacy considerations must be taken into account long after data leaves the hands of the data collector. The guidelines require that certain data collectors

> . . . take reasonable steps to protect the non-identifiable nature of data if it is distributed to non-Affiliates including not disclosing the algorithm or other mechanism used for anonymizing or randomizing the data, and obtaining satisfactory written assurance that such entities will not attempt to re-construct the data and will use or disclose anonymized data only for purposes of Online Behavioral Advertising or other uses as specified to users.

According to the IAB, reasonable steps must also be taken to ensure that any non-Affiliate to which data is transferred will also require that any other non-Affiliate given the

---

http://graphics8.nytimes.com/packages/pdf/business/20090929-Tailored_Advertising.pdf; In a 2006 TRUSTe study, 71% of respondents said that they have decided against registering or making a purchase online because those actions required them to provide information that they did not want to divulge. *See* TRUSTe, *Consumers Have False Sense of Security About Online Privacy – Actions Inconsistent with Attitudes* (December 2006) *Available At* https://clicktoverify.truste.com/about/press_release/12_06_06.php

[21] *See* Catherine Dwyer, *Behavioral Targeting: A Case Study of Consumer Tracking on Levis.com*, 15th Americas Conference on Information Systems (Aug. 2009), *available at* http://csis.pace.edu/~dwyer/research/AMCISDwyer2009.pdf.

data will respect the restrictions.[22] This requirement illustrates how Privacy by Design can be incorporated into self-regulatory principles.

Meanwhile, there is little reason that practices that are defined by technology should be monitored "by hand." Technological innovation to support industry compliance is needed as well. Multiple companies are typically involved in the targeting of a particular ad, including the advertiser in the case of retargeting, data aggregators providing data to the advertiser directly or through demand-side platforms or ad exchanges, and downstream ad networks that use behavioral data to optimize audiences as the ad is relayed to the consumer. Compliance throughout all of these data transfers should be far more automated than it is today, with compliance mechanisms built directly into ad delivery and targeting technologies.[23] The FTC should encourage innovation that will help simplify compliance without lowering standards and, more generally, should be supportive of the development of protocols that will help enable Privacy by Design.

No Silver Bullet: the need for regulation in concert with Privacy by Design

Privacy by Design promotes innovation in the privacy space as an important element of innovation more generally. But Privacy by Design should not be seen as a replacement for much-needed comprehensive, federal consumer privacy legislation or a stronger regulatory approach to privacy. Foremost, Privacy by Design relies on an assumption of good actors, working with the understanding that protecting privacy is protecting business. It is clear that not all entities operating in the online marketplace prioritize privacy. Privacy by Design, while important, should be seen as one tool in a larger toolkit that includes regulatory approaches.

CDT urges the Commission to release a new set of comprehensive FIPs and to simultaneously or subsequently release a set of guidelines with recommendations for how these FIPs can be fulfilled. These recommendations should emphasize the role of Privacy Impact Assessments, privacy threshold analyses, the integration of PETs into product development, end-to-end lifecycle protection for data, and privacy as the default or as a clear, easy-to-understand and exercisable alternative.

Efforts to encourage a Privacy by Design approach to innovation should be supplemented by a rigorous mix of self-regulation, enforcement of existing law, and enactment of a new consumer privacy statute that establishes baseline protections and gives the FTC rulemaking authority.[24] Technology and sound business practices can promote online privacy and security, but they cannot guarantee it.

---

[22] Interactive Advertising Bureau, *Self-Regulatory Principles for Online Behavioral Advertising* (July 2009) at 15-16, *available at* http://www.iab.net/about_the_iab/recent_press_releases/press_release_archive/press_release/pr-070209.

[23] There has been some encouraging work by companies in the compliance area to address some of these concerns. For example, *see* Better Advertising, http://www.betteradvertising.com/index.html (last visited Dec. 20, 2009).

[24] For a more detailed exploration of how self-regulation, enforcement of existing law, and enactment of a new consumer privacy statute that establishes baseline protections and gives the FTC rulemaking authority can, in concert, improve consumer privacy, see CDT First Roundtable Comments.

Conclusion

The past two decades have witnessed incredible innovation that has penetrated every segment of our society. Americans are increasingly moving their lives – financial, work, and personal – online, adapting Web 2.0 technologies, creating new communities, and, inadvertently or not, sharing information. But as innovation on the Internet proceeds at a rapid pace, privacy innovation has not kept up.

The Internet, and more specifically e-commerce, are ultimately built on a framework of trust;[25] as consumers become more aware of how their data is being collected and used online, a breach in the framework of trust is inevitable if regulation, industry practices, and technology fail to keep pace with consumer concerns. But if legislators, regulators, and innovators work together to buttress this framework with best practices that reflect Privacy by Design, then consumers and companies alike will discovery that privacy and innovation are not mutually exclusive, but that privacy is instead an essential element of the innovative Internet.

[25] *See* Janice Tsai, *The Impact of Salient Privacy Information on Decision-Making* (August 2009), *available at http://www.andrew.cmu.edu/user/jytsai/thesis.pdf:* "This research shows that users will pay a premium to purchase from websites that offer better privacy policies IF that privacy information is made visible and understandable."