**Before the**

**FEDERAL COMMUNICATIONS COMMISSION**

**Washington, D.C. 20554**

| | | |
|---|---|---|
| In the Matter of | ) | |
| | ) | |
| A National Broadband Plan for our Future | ) | GN Docket Nos. 09-47, 09-51, 09-137 |
| Comments – NBP Public Notice #29 | ) | |
| | ) | |
| | ) | |

**COMMENTS OF THE CENTER FOR DEMOCRACY & TECHNOLOGY: APPENDIX A**

**Refocusing the FTC's Role in Privacy Protection, Comments of the Center for Democracy & Technology In regards to the FTC Consumer Privacy Roundtable, November 6, 2009**

## Executive Summary

The Center for Democracy & Technology (CDT) welcomes the opportunity to submit comments for the FTC's first 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 for the FTC to develop and announce a comprehensive privacy protection policy for the next decade.

The FTC's current notice, choice and security regime has brought progress toward corporate compliance on privacy, but seems to have met the limits of its utility. CDT urges the FTC to finally move beyond this limited framework. Now is the time for the Commission to apply a full set of Fair Information Practice principles (FIPs) in pursuit of privacy protection. These principles, as outlined by the Department of Homeland Security in 2008, include:

- Transparency
- Individual Participation
- Purpose Specification
- Data Minimization
- Use Limitation
- Data Quality and Integrity
- Security

- Accountability and Auditing

Properly understood, FIPs constitute a comprehensive privacy framework that can guide the FTC in the 21st century. Any discussion of consumer privacy – whether in Congress, at the FTC, or within industry – must be grounded by a full set of FIPs. These principles should be reflected in any future legislation, FTC enforcement or self-regulatory efforts.

In addition, CDT makes the following specific recommendations:

1. The FTC should release an updated, comprehensive set of FIPs based on the most modern and complete model.

2. The FTC should reaffirm that violating FIPs can result in consumer harm. The Commission should pursue enforcement actions against those engaged in unfair practices, not just in the spyware space, but also in the general realm of online consumer privacy. The FTC should use these actions to highlight violations of any or all of the FIP principles, not merely notice, choice and security.

3. The FTC should use its subpoena power to acquire information about company privacy practices.

4. The FTC should encourage Congress to pass general consumer privacy legislation that is based on a full set of FIPs. Self-regulation cannot adequately protect consumer privacy when it is not girded by legal standards and more direct oversight from the FTC.

5. Whether or not specific consumer privacy legislation passes, the FTC should consider drafting its own set of consumer privacy rules if it is granted standard rulemaking authority. This would significantly clarify basic privacy expectations for consumers and businesses alike.

6. The FTC should explore the establishment of benchmarks and metrics for evaluating company privacy practices.

7. The FTC should more actively promote the continued development of privacy-enhancing technologies.

The FTC must act urgently. This Commission has a great opportunity to make its mark on history by creating a strong framework in favor of privacy, and we urge the FTC to make the most of it. Consumers deserve no less.

**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 first roundtable discussion exploring the privacy challenges posed by 21st-century technology and business practices. Now is the time for Congress and the FTC to take active roles to develop a comprehensive privacy protection policy for the next decade. We believe that these roundtable sessions will play a crucial role in developing such a framework. In the

past, the FTC has suggested that self-regulatory regimes might play an important part in protecting consumer privacy. CDT believes that self-regulation alone cannot adequately protect consumer privacy when it is not girded by legal standards and more direct oversight from the FTC. As FTC Commissioner Pamela Jones Harbour recently wrote with respect to behavioral advertising and privacy more generally, "Self-regulation cannot exist in a vacuum."[1] We thank the FTC for continuing an open dialogue about how best to move forward and we look forward to the roundtable discussions.

The collection, transfer and use of consumer data is increasingly widespread and involves such diverse services as social networking, cloud computing, online behavioral advertising, and mobile marketing. These and all other practices that pose privacy risks should be addressed as part of a comprehensive privacy agenda.[2] But despite the universality of data collection, transfer, and use, today we have a piecemeal policy approach to privacy. For example, in the behavioral advertising space, we now have multiple sets of conflicting self-regulatory principles that arguably have done little to improve the status quo.[3] Further, no metrics exist to evaluate the effectiveness of these self-regulatory efforts.

Even in the absence of such metrics, it is clear that self-regulation has generally not been a success. As FTC Chairman Jon Leibowitz warned after the Google/DoubleClick merger: "Ultimately, if the online industry does not adequately address consumer privacy through self-regulatory approaches, it may well risk a far greater response from government."[4]

CDT believes that a fair review of current business practices with regard to the use of personal and sensitive information of individuals will reveal that the time for a "far greater response from government" is now and that the response should begin with the enactment of a new consumer privacy statute that establishes baseline protections and gives the FTC clear, quick and ongoing rulemaking and civil penalty authority.[5] Self-regulation can only effectively work when consumer privacy legislation and effective

---

[1] Concurring Statement of Commissioner Pamela Jones Harbour, *Regarding Staff Report, Self-Regulatory Principles for Online Behavioral Advertising*, *available at* http://www.ftc.gov/os/2009/02/P085400behavadharbour.pdf ("Harbour Concurring Statement").

[2] *See* Harbour Concurring Statement ("I would prefer that the Commission take a more comprehensive approach to privacy, and evaluate behavioral advertising within that broader context."). Harbour further suggests "any legislation should be part of a comprehensive privacy agenda, rather than fostering the current piecemeal approach to privacy." *Id.*

[3] *See, e.g.*, Federal Trade Commission Staff Report, *Self-Regulatory Principles For Online Behavioral Advertising: Behavioral Advertising Tracking, Targeting & Technology* (Feb. 2009), *available at* http://www.ftc.gov/opa/2009/02/behavad.shtm ("Staff Report"); Network Advertising Initiative, *2008 NAI Principles: The Network Advertising Initiative's Self-Regulatory Code of Conduct* (Dec. 2008), *available at* http://www.networkadvertising.org/networks/principles_comments.asp ("NAI Principles"); Interactive Advertising Bureau, *Self-Regulatory Principles for Online Behavioral Advertising* (July 2009), *available at* http://www.iab.net/about_the_iab/recent_press_releases/press_release_archive/press_release/pr-070209 ("IAB Principles").

[4] Concurring Statement of Commissioner Jon Leibowitz, *Google/DoubleClick*, *available at* http://www.ftc.gov/os/caselist/0710170/071220leib.pdf.

[5] CDT does not believe the FTC should be the only enforcement body with privacy authority. State attorneys general and a limited private right of action with a cap on damages are also both crucial for enforcement purposes.

enforcement exist to provide it with a meaningful backbone. The FTC should also continue to pursue enforcement actions and provide guidance to industry, but with a renewed emphasis and focus on a comprehensive set of Fair Information Practice principles (FIPs). To do so, the FTC must reclaim its authority to fully enforce all of the FIPs under its unfairness jurisdiction.

Any discussion of consumer privacy – whether in Congress, at the FTC, or within industry – must be grounded by a comprehensive set of FIP principles. FIPs have been embodied to varying degrees in the Privacy Act, Fair Credit Reporting Act, and the other "sectoral" federal privacy laws that govern commercial uses of information online and offline. CDT strongly believes that the concept of FIPs has remained relevant for the digital age despite the dramatic advancements in information technology that have occurred since these principles were first developed. But the principles must be re-emphasized and refocused to be relevant and effective in the 21st century. The most recent government formulation of the FIPs offers a robust set of modernized principles that should serve as the foundation for any discussion of self-regulation or legislation in the online sector.[6] These principles, as described by the Department of Homeland Security (DHS) in 2008, include:

- **Transparency.** *Entities should be transparent and provide notice to the individual regarding its collection, use, dissemination, and maintenance of information.*

- **Individual Participation.** *Entities should involve the individual in the process of using personal information and, to the extent practicable, seek individual consent for the collection, use, dissemination, and maintenance of this information. Entities should also provide mechanisms for appropriate access, correction, and redress regarding their use of personal information.*

- **Purpose Specification.** *Companies should specifically articulate the purpose or purposes for which personal information is intended to be used.*

- **Data Minimization.** *Only data directly relevant and necessary to accomplish a specified purpose should be collected and data should only be retained for as long as is necessary to fulfill a specified purpose.*

- **Use Limitation.** *Personal information should be used solely for the purpose(s) specified in the notice. Sharing of personal information should be for a purpose compatible with the purpose for which it was collected.*

- **Data Quality and Integrity.** *Companies should, to the extent practicable, ensure that data is accurate, relevant, timely and complete.*

- **Security.** *Companies should protect personal information through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.*

---

[6] *See* 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* (Dec. 2008), *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf ("DHS FIPs").

- **Accountability and Auditing.** *Companies should be accountable for complying with these principles, providing training to all employees and contractors who use personal information, and auditing the actual use of personal information to demonstrate compliance with the principles and all applicable privacy protection requirements.*

Properly understood, FIPs constitute a comprehensive privacy framework that self-regulatory guidelines, federal legislation and FTC enforcement should all reflect. Unfortunately, most privacy schemes to date have focused only on a subset of the FIPs: some have been confined only to notice and consent.[7] Relying exclusively on notice-and-consent compliance regimes places the entire burden for privacy on the consumer to navigate an increasingly complex data environment. In most instances, little practical privacy protection is achieved by reliance on this narrow set of protections. The privacy challenges posed by the vast array of 21st-century technology and business practices require a greater emphasis on a broader set of substantive protections. Notice and consent are crucial, but they are simply not enough to adequately protect consumers today.

The FTC must act urgently. CDT encourages the FTC to refocus energy on consumer privacy issues and re-emphasize the value in comprehensively applying all of the FIP principles to protect privacy.

In Section I below we discuss the significance of a comprehensive set of FIP principles in the digital age. In Section II we provide general lessons from previous and current FTC approaches to spyware and behavioral advertising. Section III outlines specific recommendations for future FTC action.

## I. The Significance of Fair Information Practice Principles

A full set of FIPs provides a generally accepted conceptual framework for privacy that will endure amidst new technology and business practices. CDT calls for the FTC to move beyond the limited set of FIP principles it issued in 2000[8] (which have yielded a focus on only notice, consent and security in practice) and instead apply a more comprehensive set of FIPs: Transparency, Individual Participation, Purpose Specification, Data Minimization, Use Limitation, Data Quality and Integrity, Security, and Accountability and Auditing.[9] Each principle alone is not enough. We strongly believe that a renewed focus on comprehensively applying these principles will significantly help

---

[7] The *FTC's 2000 version of FIPs, for example, includes only notice, choice, access and security. See* Federal Trade Commission, *Privacy Online: Fair Information Practices in the Electronic Marketplace* (May 2000), *available at www.ftc.gov/reports/privacy2000/privacy2000.pdf ("Fair Information Practices in the Electronic Marketplace").*

[8] *See Fair Information Practices in the Electronic Marketplace (outlining the FTC's 2000 version of FIPs, which includes only notice, choice, access and security).* In selecting notice, choice, access and security as the main set of FIPs, the FTC limited its ability to work with companies and promote strong privacy rules. When an Advisory Board report came to the FTC with no conclusion on resolving online access issues, the Commission took the position that it could not act in that area, further limiting its area of protection to notice, access and security alone.

[9] *See* DHS FIPs.

to protect consumer privacy in the 21st century. In its reporting following the roundtable discussions, the FTC should express its support for these latest FIPs.

### A. The Forgotten FIPs

In 2000, the FTC issued a report to Congress outlining four core principles of privacy protection: (1) Notice/Awareness, (2) Choice/Consent, (3) Access/Participation and (4) Integrity/Security.[10] The FTC's condensed set of FIPs has been largely criticized as a watered down version of previous principles.[11] The principles focus narrowly on Web site privacy policies in practice, resulting in today's stagnant notice-and-consent framework.

Law professor Fred Cate has offered a pointed critique of the FTC privacy principles.[12] Cate describes the problems surrounding the current notice-and-consent regime, and we largely agree with his assessment of the shortcomings of the current landscape. Cate suggests that the focus on notice and choice as compliance mechanisms has led to a system consisting of "an avalanche of notices and consent opportunities" of minimal value that "are widely ignored by the public." Cate points out that neither "loading notices with exceptional detail because they will serve as contract terms [n]or reducing notices to mere cigarette-pack-like warnings has proved very informative or protective of privacy."[13]

Cate correctly argues that the most significant problem with the current FTC privacy principles is that they, in effect, transform "collection limitation, purpose specification, use limitation, and transparency into mere notice and consent" and ignore any substantive obligations.[14] In other words, the Commission has relied too heavily "on its power to prohibit 'deceptive' trade practices – i.e., practices that did not conform to published privacy policies – rather than its power to prohibit 'unfair' trade practices."[15] Now is the time for the FTC to additionally ensure "that data collection be 'fair,' that data not be used for incompatible purposes, and that data processing operations generally be open."[16] We believe a greater emphasis on substantive privacy protections can be achieved by robust application of the full set of FIP principles.[17] Cate does not, however, address the FTC's many actions on security, including significant cases like Microsoft Passport and the ChoicePoint data breach. While these are important cases that move

---

[10] *See* Fair Information Practices in the Electronic Marketplace.

[11] *See, e.g.*, Fred H. Cate, *The Failure of Fair Information Practice Principles*, *in* CONSUMER PROTECTION IN THE AGE OF THE 'INFORMATION ECONOMY' 341 (Jane K. Winn ed., 2006) ("The Failure of Fair Information Practice Principles"); Robert Gellman, *Fair Information Practices: A Basic History* (Dec. 2008), *available at* http://*bobgellman.com/rg-docs/rg-FIPshistory.pdf.*

[12] *See* The Failure of Fair Information Practice Principles.

[13] *Id.* at 358, 362. "Notice and choice requirements often create the illusion, but not the reality, of meaningful consumer choice." *Id.* at 364.

[14] *Id.* at 355-56. Cate does not suggest that notice and choice are simply irrelevant; rather, he believes our approach to privacy should not rely on notice and choice for all purposes. *See id.* at 342. CDT agrees with Cate here.

[15] *Id.* at 351.

[16] *Id.* at 356.

[17] While Cate does a thorough and commendable job detailing the failure of the current FIPs regime embraced by the FTC, we disagree with Cate's conclusion that a harms-based model based on a set of new FIPs is a better approach.

industry in the right direction on protecting consumer security online, they only offer a limited set of protections.

To enforce a full set of FIPs absent broader rulemaking authority, the FTC must rely on its power to prohibit unfair trade practices. Only recently has the Commission begun to file complaints based on allegations of unfair privacy practices as opposed to only deceptive practices. The Commission has continued to favor cases that hinge on procedural deceptive practices instead of the substantive unfair practices and this has contributed to a regime in which procedural compliance mechanisms are favored over a full set of FIPs. The FTC needs to reclaim and re-emphasize its power under Section 5 of the FTC Act to prohibit unfair trade practices and, in doing so, stress the importance of the forgotten FIP principles.

The crux of any unfairness complaint lies in determining what qualifies as "unfair." Section 5 of the FTC Act defines a practice as unfair if the injury to consumers is substantial, not outweighed by countervailing benefits, and not reasonably avoidable by the consumers.[18] While some have argued that privacy "harms" should be defined as tangible injury, we strongly agree with FTC Consumer Protection Bureau Director David Vladeck's notion of a more expansive view of harm as a potentially intangible concept that goes beyond monetary loss to include violations of dignity.[19] Having established an appropriate conception of harm, CDT believes that the FTC will quickly find the privacy violations regularly occurring online blatantly unfair.

## II. Examining FIPs at Work: Recent FTC Enforcement Actions Demonstrate a Path Forward

This section further explores how a full set of FIPs can be effectively implemented as part of a comprehensive privacy agenda. We first provide examples of how the FTC has used its authority to police unfair practices in the spyware space and how this authority should be exercised in the general consumer privacy space. We then offer concrete lessons from the current notice, choice and security regime and present a comparison with the privacy protections necessitated by adherence to a comprehensive set of FIPs. Third, we illustrate the value of applying a full set of FIPs to unfair and deceptive behavioral advertising practices.

### A. The FTC's Unfairness Jurisdiction and Consumer Privacy – A Lesson from Spyware Enforcement

As the FTC continues its efforts to protect consumer privacy, it should look to its successful experience fighting spyware for guidance. Over the past six years, the FTC

---

[18] *See* Section 5(n) of the FTC Act, 15 U.S.C. § 45(n), *added by* The Federal Trade Commission Act Amendments of 1994, Pub. L. No. 103-312.

[19] *See* Stephanie Clifford, *Fresh Views at Agency Overseeing Online Ads*, N.Y. TIMES, Aug. 4, 2009, *available at* http://www.nytimes.com/2009/08/05/business/media/05ftc.html (In discussing the Sears case, Vladeck said, "'There's a huge dignity interest wrapped up in having somebody looking at your financial records when they have no business doing that'"). Vladeck further describes this dignity interest in an interview with the NYTimes.com: "I think that we in society do place a value, although not easily quantifiable, on anonymity." *See An Interview with David Vladeck of the F.T.C.*, NYTIMES.COM, Aug. 5, 2009, http://mediadecoder.blogs.nytimes.com/2009/08/05/an-interview-with-david-vladeck-of-the-ftc/ (last visited Nov. 5, 2009) ("An Interview with David Vladeck").

has taken the lead law enforcement role in fighting spyware, one of the most serious threats to the Internet's continued usefulness, stability and evolution. The FTC brought its first spyware complaint in 2004, when it pursued a petition filed by CDT against Seismic Entertainment, a network of deceptive adware distributors and their affiliates. The FTC's complaint and the 2006 settlement of the case centered around three unfairness counts against Seismic.[20] The FTC was clear: some online acts so tip the harm-benefit balance that even absent deception, they are unfair to consumers. The case thus reaffirmed the role of the FTC's unfairness jurisdiction in protecting consumers from substantive harm on the Internet.

In addition to the Seismic case, the FTC has brought twelve spyware enforcement actions and, in doing so, has played a key role in stemming the tide of this Internet scourge. But as the FTC has laid the groundwork for controlling malicious spyware, other online threats to consumer privacy have increased considerably. As the FTC shifts its focus from spyware to broader privacy threats, it should look toward the precedents it created in its spyware cases, many of which directly bear on broader consumer privacy threats.

For example, no fewer than eight out of the Commission's thirteen spyware cases have dealt with the practice of tracking Internet activity for the purposes of serving targeted advertising,[21] and in three of those cases this tracking was considered an "unfair" act.[22] In the Enternet Media case, for example, the FTC took issue with software code that "tracks consumers' Internet activity," claiming that this practice was part of an unfair act that was "likely to cause substantial injury to consumers."[23] By recognizing that consumer tracking can constitute an unfair act, the FTC took an important step toward recognizing other kinds of harms.

As it considers new threats to consumer privacy, the FTC should continue to bring unfairness cases: unfair practice rulings were an integral part of the Commission's successful fight against spyware and are necessary to effectively ensure strong online consumer privacy protections. CDT believes the time is ripe for the FTC to explicitly acknowledge the harms caused by unfair privacy practices in general. The FTC will

---

[20] *See* Complaint at 10-13, FTC v. Seismic Entm't, No. CV-00377 (D.N.H. Oct. 6, 2004), *available at* http://www.ftc.gov/os/caselist/0423142/041012comp0423142.pdf ("Seismic Entm't") (The three counts included: (1) Unfairly Changing Consumers' Web Browsers; (2) Unfairly Installing Advertising and Other Software Programs; and (3) Unfairly Compelling Purchase of "Anti-Spyware" Software).

[21] For a list of cases, see Federal Trade Commission Information on Spyware, Enforcement Actions, http://www.ftc.gov/bcp/edu/microsites/spyware/law_enfor.htm (last visited Nov. 5, 2009). *See also* Complaint, In the Matter of Sears Holdings Management Corporation, No. C-4264 (Aug. 31, 2009), *available at* http://www.ftc.gov/os/caselist/0823099/090604searscmpt.pdf; Complaint, FTC v. Cyberspy Software LLC, No. CV-01872 (M.D. Fla. Nov. 5, 2008), *available at* http://www.ftc.gov/os/caselist/0823160/081105cyberspycmplt.pdf ("Cyberspy Software LLC"); Complaint, In the Matter of Sony BMG Music Entm't, No. C-4195 (June 29, 2007), *available at* http://www.ftc.gov/os/caselist/0623019/0623019cmp070629.pdf ("Sony BMG Music Entm't").

[22] *See* Complaint, FTC v. Enternet Media, Inc., No. CV05-7777 (C.D. Cal. Nov. 4, 2005), *available at* http://www.ftc.gov/os/caselist/0523135/051110amndcomp0523135.pdf ("Enternet Media, Inc."); Amended Complaint, FTC v. ERG Ventures, LLC et al., No. CV-00578 (D.Nev. May 23, 2007), *available at* http://www.ftc.gov/os/caselist/0623192/070523ergventmediamotoramndcmplt.pdf ("ERG Ventures, LLC et al."); Cyberspy Software LLC.

[23] Enternet Media, Inc., at 14-15.

successfully meet the challenges of the digital age only if it begins to move beyond its notice, choice, and security regime and protect all of the FIPs under its unfairness jurisdiction.

### B. Redefining "User Control" – The Need For More Substantive Privacy Protection

The FTC's spyware principles revolve around the concept of user control – ensuring that consumers are in command of their computers, what gets stored on those computers, and how those computers can be accessed by Internet businesses. The FTC has not hesitated to act within its unfairness jurisdiction against a wide range of behaviors that jeopardize user control.[24]

In pursuing privacy protections more generally, the FTC should broaden its conception of "user control" from click-of-the-button "consent" to a set of consumer rights and company responsibilities that together fortify and protect the decisions that consumers make online. The current opt-in/opt-out consent paradigm at best only gives consumers control over their data at the point of collection. Long after data is collected, it lives in a Wild West of shared and sold personal profiles and databases that give consumers no control over how their identities will be tracked and used. As Commissioner Pamela Jones Harbour has said, "Once data is shared, it cannot simply be recalled or deleted – which magnifies the cumulative consequences for consumers, whether they realize it or not."[25]

An analysis of the FTC's 2009 settlement with Sears highlights the need to move beyond today's notice and consent regime. Between 2007 and 2008, Sears encouraged users to download tracking software on their computers.[26] This software monitored consumers' activities for clues about both online and offline behavior, peering into online secure sessions and culling information from consumers' email subjects and recipients, online bank statements, drug prescription records, video rental records, and similar histories and accounts. Although Sears offered customers a $10 coupon to download the software, the Commission nonetheless brought a complaint, concluding that consumers

---

[24] *See, e.g.*, Cyberspy Software LLC; Seismic Entm't; Sony BMG Music Entm't; Enternet Media, Inc.; ERG Ventures, LLC et al.; Complaint, FTC v. Odysseus Marketing, Inc. No. CV-00330 (D.N.H. Oct. 5, 2005), *available at* http://www.ftc.gov/os/caselist/0423205/050929comp0423205.pdf; Complaint, FTC v. Digital Enters., Inc., No. CV06-4923 (C.D. Cal. Aug. 8, 2006), *available at* http://www.ftc.gov/os/caselist/0623008/060808movielandcmplt.pdf; Complaint, In the Matter of Zango, Inc., No. C-4186 (Mar. 7, 2007), *available at* http://www.ftc.gov/os/caselist/0523130/0523130c4186complaint.pdf; Complaint, In the Matter of DirectRevenue LLC, No. C-4194 (June 26, 2007), *available at* http://www.ftc.gov/os/caselist/0523131/0523131cmp070629.pdf.

[25] Harbour Concurring Statement.

[26] Between 2007 and 2008, 15 of every 100 visitors to sears.com or kmart.com were presented with a pop-up window that offered the opportunity to "talk directly to a retailer" and become part of "a place where your voice is heard and your opinion matters, and what you want and need counts!" No mention was made that this "opportunity" also installed detailed tracking software on the user's computer. Customers who asked for more information were offered a $10 coupon in exchange for downloading – and keeping on their computer for at least one month – software from Sears or K-mart that would allow them to become "part of something new, something different[.]" This software monitored consumers' online activities, including email messages, online banking sessions, and other similar activities. Customers consented to the download and tracking by agreeing to a lengthy terms of service agreement that showed up at the end of a long registration process. The agreement was presented in a small "scroll box"; consumers could only see ten lines of the policy at a time and not until the 75th line could the user find any description of the invasive tracking. *See* Complaint, In the Matter of Sears Holdings Management Corporation, No. C-4264 (Aug. 31, 2009), *available at* http://www.ftc.gov/os/caselist/0823099/090604searscmpt.pdf.

are harmed by privacy invasions in and of themselves. Companies must be certain that consumers clearly understand when they are selling their privacy.

The FTC's complaint focused on the fact that the extensive tracking undertaken by the software was neither accurately represented nor adequately disclosed by language buried deep in the Privacy Statement and User License Agreement (PSULA).[27] The complaint represents broader recognition that few consumers read or understand these kinds of disclosures about online data collection and use practices.[28] As David Vladeck told *The New York Times*, "the empirical evidence we're seeing is that disclosures on their own don't work, particularly disclosures that are long, they're written by lawyers, and they're written largely as a defense to liability cases. Maybe we're moving into a post-disclosure environment."[29]

But in its guidance to Sears about how the company could legally encourage users to download tracking software, the FTC missed an opportunity to materially improve comprehensive privacy protections available to consumers. The Commission required that "if Sears advertises or disseminates any tracking software in the future, it must clearly and prominently disclose the types of data the software will monitor, record, or transmit" and "obtain express consent from the consumer to the download or installation of the Tracking Application." The disclosure, the FTC concluded, must occur separately from any general terms of service or user license agreement and, if data will be accessed by a third party, must include a notification that data will be available to a third party; consumer consent should involve clicking a button that is not pre-selected as a default.[30] With its decision to merely require that one ineffective form of disclosure and consent be replaced by a slightly improved version, the FTC failed to ensure holistic privacy protections for the future: even the clearest of disclosures cannot, on their own, protect consumers from privacy risks or return meaningful control back to the consumer.[31]

---

[27] *See id.*

[28] U.S. District Court Judge Sterling Johnson Jr., recently ruled that simply posting a link to onerous terms and conditions on a website is not binding for the consumer. His reasoning? The evidence that any consumers actually read these policies is scant. *See* Wendy Davis, *Court Rules Overstock Can't Enforce 'Browsewrap' Agreement*, MediaPost Blogs (Sept. 14, 2009), http://www.mediapost.com/publications/?fa=Articles.showArticle&art_aid=113404 (last visited Nov. 3, 2009). Further, in a large-scale study of consumer attitudes toward behavioral advertising 62% of respondents believed that "If a website has a privacy policy, it means that the site cannot share information about you with other companies, unless you give the website your permission." *See* Joseph Turrow, Jennifer King, Chris Jay Hoofnagle, Amy Bleakley & Michael Hennessey, *Contrary to What Marketers Say, Americans Reject Tailored Advertising and Three Activities that Enable It* (Sept. 2009), *available at* http://graphics8.nytimes.com/packages/pdf/business/20090929-Tailored_Advertising.pdf.

[29] *See* An Interview with David Vladeck (Vladeck also remarked that given the "disclosures" complexity, "I'm not sure that [so-called] consent really reflects a volitional, knowing act.").

[30] *See* Agreement Containing Consent Order at 4, In the Matter of Sears Holdings Management Corporation, No. 082 3099 (June 4, 2009), *available at* http://www.ftc.gov/os/caselist/0823099/090604searsagreement.pdf. Sears was also ordered to cease data collection, delete collected data, and provide various forms of notification and support to customers who have already downloaded the tracking software. *Id.*

[31] *See* Joseph Turrow, Jennifer King, Chris Jay Hoofnagle, Amy Bleakley & Michael Hennessey, *Contrary to What Marketers Say, Americans Reject Tailored Advertising and Three Activities that Enable It* (Sept. 2009), *available at* http://graphics8.nytimes.com/packages/pdf/business/20090929-Tailored_Advertising.pdf.

Despite the monumental privacy invasion involved in the Sears case, we would not be surprised to see the same practices used in the future by companies that track consumers just as insidiously but provide marginally clearer notification of their practices. Indeed, a company in similar circumstances may be able to sell consumers' personal information to others with no ability to revoke that information from the buyer if consumers later change their mind. Such a company would merely need to be a little more upfront about its intentions than Sears was in this case. This is the ultimate failure of the notice, consent and security regime.

On the other hand, had the FTC taken the opportunity to outline a multi-tiered privacy framework based on a full set of FIP principles that Sears and other companies must work within, the Commission would have taken a much more significant step toward meaningful protection of consumer privacy.

Consider, instead, what might have transpired had Sears applied the FIPs principle of Transparency – which is often equated with "notice" but is indeed much broader – when developing its software. Transparency would require consumers have access to the personal information entities have been collecting about them. It is difficult to imagine that Sears would have collected and stored sensitive health and financial information if they then had to let consumers see the personal profiles being constructed about them (like the one registered Google and BlueKai users can access).[32] The Individual Participation and Data Quality and Integrity principles reinforce the need for this access, as they require that consumers have the tools to correct mistakes or challenge information reported in these profiles. After all, the best way to ensure that data is accurate is to provide consumers with access to review and correct it.

Ensuring data quality is imperative, for data collected by one entity is often shared or sold to third parties for secondary uses. Sharing or selling consumer data, or using it for price discrimination, employment decisions, or to make credit or insurance decisions, is a serious concern and often directly harmful to consumers; this data can be even more harmful when it is inaccurate.

But profile access alone is not a strong enough check to protect consumers against secondary uses of personal data. Full implementation of the Data Minimization, Purpose Specification, and Use Limitation principles would help provide this check. The Data Minimization principle, for example requires that entities only collect data "that is directly relevant and necessary to accomplish the specified purpose(s) and only retain [that data] for as long as is necessary to fulfill the specified purpose(s)."[33] It is hard to believe that consumer banking information is "directly relevant and necessary" to Sears' business model. And if such data were relevant, the Purpose Specification principle would have forced Sears to "specifically articulate" this relevance; we imagine that being required to publicly announce alarming data-use practices might act as a prophylactic for insidious

---

[32] *See* Google Ads Preferences, http://www.google.com/ads/preferences (last visited Oct.30, 2009); BlueKai Registry - Consumer Preferences, http://tags.bluekai.com/registry (last visited Oct. 30, 2009). But Google and BlueKai do not show the consumer the underlying data on which the profile is based – they show the inferences drawn from the data, but they do not show what data is being collected and retained, where it was collected, and what partners, if any, it is being shared with. In other words, although a positive step, more work needs to be done.

[33] DHS FIPs.

tracking. The Use Limitation principle dovetails with Purpose Specification to protect against illegitimate uses of collected data. The data retention limits outlined within the Data Minimization principle provide an additional check: if data is deleted or aggregated then it cannot be used in a way that is harmful to the individual consumer.[34]

Of course, absent security measures to protect collected data and accountability measures put in place by individual companies, trade associations, the FTC, or Congress, all of these promises could prove empty. But with such measures firmly in place, these individual FIP principles can work in concert to buttress stronger privacy protections.

### C. Application of FIPs to Online Behavioral Advertising

The Sears case involved elements of both spyware and its cousin, behavioral advertising. Behavioral advertising, which has already garnered significant attention from the FTC, continues to be a concern from a consumer privacy perspective.

Massive increases in data processing and storage capabilities have allowed advertisers to track, collect and aggregate information about consumers' Web browsing activities and compile individual profiles 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 sophisticated new behavioral advertising models are deployed – including models built around data-collecting Internet Service Providers (ISPs) – it is vital for legal protections to keep pace with these developments.

Although current self-regulatory efforts continue to expand and greatly improve – the FTC has issued self-regulatory guidelines, as have the Network Advertising Initiative (NAI)[35] and the Interactive Advertising Bureau (IAB),[36] – they fall short of adequately protecting consumers in this space. The reason is two-fold: the protections built into the self-regulatory principles are insufficient and the regulating bodies have failed to ensure compliance.

---

[34] For example, Yahoo! recently changed its data retention policy so that it now anonymizes all data on its server logs (including search results, page views, page clicks, ad views and ad clicks) after three months. Yahoo!'s decision was based on its determination that the purpose for which the personally identifiable search data was initially collected would not be served by data more than three months old. *See* Press Release, Yahoo!, Yahoo! Sets New Industry Privacy Standard with Data Retention Policy (Dec. 17, 2008), *available at* http://yhoo.client.shareholder.com/press/releasedetail.cfm?ReleaseID=354703. The way in which Yahoo! goes about truly making this data anonymous requires additional discussion. *See, e.g.*, Kevin Bankston, Electronic Frontier Foundation Deeplinks Blog, *Yahoo To Anonymize Logs After 90 Days, Compared to Google's 9 Months*, Dec. 17, 2008, http://www.eff.org/deeplinks/2008/12/yahoo-anonymize-logs-after-90-days-compared-google ("Fully anonymizing IP addresses and cookie data can be tricky"). Nevertheless, this is an encouraging development and has opened a debate on how much data is enough. Minimizing collection and aggregation of consumer data can significantly reduce the privacy risks associated with online consumer profiling without decreasing the efficacy of advertising efforts. *See* Jun Yan, Ning Liu, Gang Wang, Wen Zhang, Yun Jiang & Zheng Chen, *How much can Behavioral Targeting Help Online Advertising* (2009), *available at* http://www2009.eprints.org/27/1/p261.pdf.

[35] NAI Principles.

[36] IAB Principles.

While the FTC's guidelines represented a major step forward toward better policies on behavioral advertising, the protections they provide are limited. The guidelines are organized along principles of "Transparency and Consumer Control," "Reasonable Security, and Limited Data Retention for Consumer Data," "Affirmative Express Consent for Material Changes to Existing Privacy Promises," and "Affirmative Express Consent to (or Prohibition Against) Using Sensitive Data for Behavioral Advertising."[37] Instead of setting out a broad, comprehensive self-regulatory framework with detailed guidance for behavioral advertisers of different kinds built in, the FTC focused on this narrow set of requirements, further contributing to a behavioral advertising ecosystem that lacks substantive limitations on data collection and uses, means for ensuring data quality, and mechanisms for accountability.

As one example, the FTC does not require behavioral advertisers to provide consumers with access to their behavioral profiles (nor does the IAB).[38] Fortunately, in the realm of profile access, Google and BlueKai decided to exceed the requirements of all the guidelines. This may be due in part to the FTC's encouragement of industry creativity, but not all of industry can be counted on to be so inventive in the absence of higher standards. The Commission could have made this part of the guidance from the start.

None of the three sets of guidelines explicitly provide for Use Limitation or, in the spirit of the Data Minimization principle, tie data retention to the purpose for which the data was originally collected. Accountability procedures are also lacking. Because they emphasize notice, consent, and security regimes over a comprehensive protective framework, the FTC, NAI, and IAB principles are all insufficient to return meaningful control to users.

As it continues to engage with industry on self-regulatory efforts, the FTC should use the eight FIP principles as the foundation for evaluating behavioral advertising practices. Self-regulatory principles that include a full set of FIPs would address many of the gaps in the current behavioral advertising ecosystem and also provide a common vocabulary as the different sets of guidelines begin to see implementation. These principles should further apply to behavioral advertising conducted not only through traditional technologies but also through ISPs, toolbars, and other technologies (as is done in the IAB principles).

We are skeptical, however, that even the most comprehensive self-regulatory framework would effectively police behavioral advertising practices. First, a self-regulatory system that relies on trade associations to provide implementation and accountability guidelines is clearly incomplete: the activities of non-members will remain unregulated. No self-regulatory system is likely to cover or be enforced against all entities, especially when new participants so regularly enter and leave the scene. Second, a confederated set of notifications, mechanisms for consent, and principles that guide data collection and use will only confuse consumers who do not understand what they have or have not opted out of or opted into and why a visit to a Web site forces them into relationships not only with the myriad advertisers and advertising networks servicing that site but also with the

---

[37] Staff Report.

[38] The NAI does call for limited access to profiles, but it does not provide much detail about what such access would mean. *See* NAI Principles at 9.

NAI and the IAB. Third, self-regulation is simply an improper mechanism for true consumer protection. The trade associations continue to define the types of activities that are and are not covered by self-regulatory guidelines based on how they structure their business contracts rather than how the activities impact consumer privacy.[39] Furthermore, implementation of self-regulatory principles has been slow at best.

When the FTC principles were released in 2008, Commissioner Harbour wrote in her concurring statement:

> Industry consistently argues that self-regulatory programs are the best way to address privacy concerns, but the evidence is mixed at best. Self-regulation has not yet been proven sufficient to fully protect the interests of consumers with respect to behavioral advertising specifically, or privacy generally.[40]

Both the FTC Staff Report that outlined the FTC self-regulatory principles and Commissioner Leibowitz's concurring statement echo this concern about the effectiveness of self-regulation.[41]

CDT strongly believes that it is time for the FTC to play a larger role to ensure that consumer interests are fully protected here. The FTC should rely on some of the precedents it established in the spyware cases and it should challenge companies engaging in unfair behavioral advertising practices. The Commission should further use these cases as opportunities to establish a more comprehensive framework for addressing broader privacy concerns – a framework based on a full set of FIPs.

## III. CDT's Recommendations

In 2008, Chairman (then-Commissioner) Leibowitz warned that despite the FTC's efforts to encourage self-regulation, consumer privacy protections remain remarkably weak:

> Indeed, despite a spotlight on e-commerce and online behavioral marketing for more than a decade, to date data security has been too lax, privacy

---

[39] The IAB and NAI, for example, do not apply to third-party entities that are collecting data from sites with which they are affiliated. For instance, DoubleClick, which is owned by IAB member company Google, could track individuals on Web sites owned by Google – such as Gmail, Google Books, YouTube, and Blogspot – without providing any notifications or mechanisms for control and regardless of the information's sensitive nature. *See* IAB Principles at 10-11. The NAI also distinguishes between "Online Behavioral Advertising," "Multi-Site Advertising" and "Ad Delivery & Reporting." According to the NAI's definition, Online Behavioral Advertising refers only to the practice of using collected data to "categorize likely consumer interest segments." So-called Multi-Site Advertising covers a much broader set of data collection and use practices that also pose privacy risks. However, while the NAI has extended nearly all of its principles (i.e., notice, transfer and service restrictions, access, reliable sources, security, and data retention) to cover Online Behavioral Advertising and Multi-Site Advertising, the NAI has neither established a choice requirement for Multi-Site Advertising nor specifically applied its use limitations principle to Multi-Site Advertising. *See* NAI Principles at 4.

[40] Harbour Concurring Statement.

[41] *See* Concurring Statement of Commissioner Jon Leibowitz, *Regarding Staff Report, Self-Regulatory Principles for Online Behavioral Advertising, available at* http://www.ftc.gov/os/2009/02/P085400behavadleibowitz.pdf ("Leibowitz Concurring Statement") ("Industry needs to do a better job of meaningful, rigorous self-regulation or it will certainly invite legislation by Congress and a more regulatory approach by our Commission. Put simply, this could be the last clear chance to show that self-regulation can – and will – effectively protect consumers' privacy in a dynamic online marketplace.").

> policies too incomprehensible, and consumer tools for opting out of targeted advertising too confounding. Industry needs to do a better job of meaningful, rigorous self-regulation or it will certainly invite legislation by Congress and a more regulatory approach by our Commission.[42]

CDT believes that although progress has been made in expanding self-regulatory efforts in areas such as online behavioral advertising, fully protecting consumer privacy interests online requires a rigorous mix of self-regulation, enforcement of existing law, development of technical tools, and enactment of a new consumer privacy statute that establishes baseline protections and gives the FTC rulemaking authority. Effectively implementing this mix of protections will require the FTC to take a number of interrelated steps:

1) *The FTC should release an updated, comprehensive set of FIPs based on the most modern and complete model.*

Through its reports, workshops, and guidelines, the FTC has played an important role in promoting good privacy practices online. We urge the Commission to continue to promote industry best practices through the development of a comprehensive set of FIPs. As we have detailed in these comments, the FTC's 2000 FIPs are insufficient in the present environment, one that sees consumer information collected and used in increasingly insidious ways. In the FTC's reporting following the roundtable discussions, the Commission should issue a new set of FIPs based on the most modern set, those released by DHS. Future guidelines and principles on topics such as behavioral advertising should be built around these FIPs.

2) *The FTC should reaffirm that violating FIPs can result in consumer harm. The Commission should pursue enforcement actions against those engaged in unfair practices, not just in the spyware space, but also in the general realm of online consumer privacy. The FTC should use these actions to highlight violations of any or all of the FIP principles, not merely notice, choice and security.*

The FTC has demonstrated that it can effectively pursue businesses engaged in unfair and deceptive practices when serious privacy threats are involved. The Commission has taken the lead law enforcement role in fighting spyware, successfully combating one of the most serious threats to the Internet's continued usefulness, stability and evolution. As the Commission continues its fight against privacy invasions through enforcement actions, it should focus on applying its unfairness jurisdiction in privacy cases, establishing the violation of dignity as a harm in its own right that may be inflicted by invading privacy, and framing decisions around a modern, comprehensive set of FIPs. As it did with spyware, the FTC should encourage companies to understand the broad principles guiding its enforcement actions.

3) *The FTC should use its subpoena power to acquire information about company privacy practices.*

---

[42] *Id.*

There is surprisingly little transparency about how companies are collecting, using, sharing, and selling consumer data. As the Sears case demonstrated, companies are not limiting their data collection to the observation of unencrypted Web browsing habits; some are tracking emails, secure sessions, prescription information, and banking activities.

But as Chairman Leibowitz wrote in 2008, although the FTC has gathered a smattering of evidence showing that a few companies have engaged in these unsavory practices, the industry has been remarkably unforthcoming with information about how it treats personal data collected online:

> The possibility that companies could be selling personally identifiable behavioral data, linking click stream data to personally identifiable information from other sources, or using behavioral data to engage in price discrimination or make credit or insurance decisions are not only unanticipated by most consumers, but also potentially illegal under the FTC Act. Industry's silence in response to FTC staff's request for information about the secondary uses of tracking data is deafening. As a result, the Commission may have to consider using its subpoena authority under Section 6(b) of the FTC Act to compel companies to produce it.[43]

Protecting consumers' privacy requires a complete understanding of how their privacy is being violated – an understanding we do not yet have. The FTC should act on Chairman Leibowitz's threat and force companies to account for their uses of consumers' personal information.

The need for the FTC to exercise its subpoena power is even clearer in the context of Deep Packet Inspection (DPI), a practice in which technologies are employed that potentially allow ISPs and other intermediaries to analyze all of the Internet traffic of millions of users simultaneously, often for the purposes of collecting data for the targeting of behavioral advertisements. The privacy risks inherent in DPI cannot be overstated, but relatively little is known about the information ISPs are collecting and examining, how long that information is retained, and how that information is being used or shared.[44]

4) *The FTC should encourage Congress to pass general consumer privacy legislation that is based on a full set of FIPs. Self-regulation cannot adequately protect consumer privacy when it is not girded by legal standards and more direct oversight from the FTC.*

Despite the unprecedented challenges to privacy in the modern environment, the United States still has no comprehensive law that spells out consumers' privacy rights in the

---

[43] Leibowitz Concurring Statement. In 2007, Leibowitz also wrote: "If we do not obtain the information we need to put some meat on the proposed self-regulatory framework, the Commission should consider using its subpoena authority under Section 6(b) of the FTC Act to compel companies to produce data about their online practices." Concurring Statement of Commissioner Jon Leibowitz, *Google/DoubleClick, available at* http://www.ftc.gov/os/caselist/0710170/071220leib.pdf.

[44] *See The Privacy Implications of Deep Packet Inspection: Hearing Before the Subcomm. on Communications, Technology and the Internet of the H. Comm. on Energy and Commerce*, 111th Cong., 1st Sess. (Apr. 23, 2009) (statement of Leslie Harris, President and Chief Executive Officer, Center for Democracy & Technology).

commercial marketplace. Instead, a confusing patchwork of distinct standards has developed over the years, with highly uneven results and many gaps in coverage. Consumers and companies alike deserve consumer privacy legislation that clarifies the general rules for all parties. Such legislation should include broad FTC rulemaking authority under Section 5 of the FTC Act that will enable the Commission to act with greater flexibility and within a more reasonable timeframe than it can today under its Magnuson-Moss rulemaking authority. Consumer privacy legislation should clarify how it applies to industries whose activities fall outside the FTC's scope.

The FTC should not, however, be the only enforcement body for privacy. State attorneys general have an important role to play in policing consumer privacy violations.[45] A limited privacy right of action with a cap on damages would also be helpful for enforcement purposes. Consumer privacy legislation should provide for both of these enforcement mechanisms.

Finally, any consumer privacy legislation should codify the fundamentals of the most modern, comprehensive set of FIPs.

5) *Whether or not specific consumer privacy legislation passes, the FTC should consider drafting its own set of consumer privacy rules if it is granted standard rulemaking authority. This would significantly clarify basic privacy expectations for consumers and businesses alike.*

General consumer privacy legislation may not pass in Congress in the near future. However, in the absence of general consumer privacy legislation, the FTC may still have the opportunity to craft a strong privacy protection framework on its own, especially if Congress grants the FTC standard rulemaking authority, as many other agencies already have under the Administrative Procedure Act. This grant has been included in proposed legislation for consumer financial protection and to reauthorize the FTC and has been supported by the Commission.

Standard rulemaking authority would give the FTC the tools it needs to craft its own comprehensive consumer privacy rules and to make enforcement of the rules meaningful, even in the absence of general consumer privacy legislation. Under these new powers, the FTC should explore the creation of rules based on a comprehensive set of FIPs and should clearly establish that violating these FIPs can amount to a consumer harm. Such rules would clarify the basic expectations of privacy for both consumers and companies.

6) *The FTC should explore the establishment of benchmarks and metrics for evaluating company privacy practices.*

---

[45] The FTC can, however, influence the way state law enforcement handles privacy invasions. For example, the principles outlined by the FTC in its battles against spyware have helped to direct state law enforcers who have already begun to take on spyware cases. The spyware space is fraught with gray areas and the FTC's guiding principles provide a simple, understandable baseline for current and future law enforcers as they wade into spyware issues with which they may be unfamiliar. In this way, the leadership of the FTC has been a vital component in expanding the nationwide pool of law enforcement resources dedicated to combating spyware.

One of the biggest challenges in establishing a framework for protecting consumer privacy is creating benchmarks and metrics for measuring whether privacy protections are in fact improving.

In particular, there has been too much focus on compliance efforts and not enough time spent attempting to find actual performance measures. For example, in the past, the FTC has evaluated success by counting the number of privacy policies online and the comprehensiveness of these policies,[46] but long privacy policies are not equivalent to better privacy protections. One obvious interim step is to measure the quality of compliance (that is, measuring whether policies actually protect privacy rather than simply attempting to indemnify a company with bad practices), however, even that type of measure does not really examine whether privacy is better protected more generally.

The FTC's annual report on the number of identity is one example of a useful metric, and we believe that with detailed research the FTC can construct more ways to measure how well industries are protecting user privacy. Benchmarks are necessary for accountability and performance metrics are the best tools we have to see if efforts in this space are indeed succeeding. This same discussion is occurring within the federal government, as government agencies seeks to marry security and privacy measures; the FTC should work with these agencies to find the best set of solutions to this challenge.[47] The Commission should also conduct a roundtable and produce a report on this specific topic of developing performance standards on privacy.

7) *The FTC should more actively promote the continued development of privacy-enhancing technologies.*

The Commission has in the past suggested that privacy-enhancing technologies play an important role in protecting consumers' privacy online. The last time this was done in detail was 1996 and in the limited area of notice and choice.[48] More recently, the FTC has relegated promotion of these important tools to specific issue areas. For example, former Chairman Deborah Platt Majoras actively supported the adoption of user-control technologies such as anti-spyware programs.[49] These technologies were essential in sustaining a victory over spyware. This type of success needs to be more widely realized.

With respect to consumer privacy in general, as with spyware, efforts to return control to users will ultimately fail unless they are bolstered by technological solutions.

---

[46] *See Fair Information Practices in the Electronic Marketplace*.

[47] *See, e.g.*, *Protecting Personal Information: Is the Federal Government Doing Enough?: Hearing Before the S. Comm. on Homeland Security & Governmental Affairs*, 110th Cong., 1st Sess. (June 18, 2008) (statement of Ari Schwartz, Vice President, Center for Democracy & Technology).

[48] *See* Federal Trade Commission Staff Report. *Public Workshop on Consumer Privacy on the Global Information Infrastructure* (Dec. 1996), *available at* http://www.ftc.gov/reports/privacy/Privacy1.shtm (A section of this report was entitled "Technologies to Enhance Notice and Consumer Choice Online").

[49] *See* Chairman Deborah Platt Majoras, *Finding the Solutions to Fight Spyware: The FTC's Three Enforcement Principles*, Anti-Spyware Coalition Public Workshop (Feb. 9, 2006), *available at* http://www.ftc.gov/speeches/majoras/060209cdtspyware.pdf ("I applaud the efforts that industry has made to develop and deploy new technologies to combat spyware, and I hope that these efforts are just the beginning.").

Several commendable efforts have already been made to help Internet users exercise a semblance of control over the collection, use, and transfer of personal information. Web browsers have long included features that allow users to control cookies and other mechanisms for collecting information about Internet users. Electronic cash allows the purchase of goods online relative anonymity. Encryption software and services can protect data in storage or transit. For situations requiring an extra level of anonymity, technical means have been developed to protect privacy by cloaking information likely to reveal identity or decoupling this identity information from the individual's actions and communications; these tools, while not perfect, make it harder to identify individuals as they browse the Web.[50]

Like Chairman Majoras, Commissioner Harbour has also actively supported the development of technologies that help protect user privacy and anonymity online[51] and we urge the Commission to further encourage the development of such products. In a technology age, innovation should be an integral part of any efforts to protect consumer privacy.

The Commission should join privacy and data protection commissioners around the world in holding workshops and more actively and more directly promoting privacy enhancing technologies.[52]

**Conclusion**

Privacy is an issue that will define the use of technology in the 21st century. Some have suggested that privacy is already dead,[53] but in reality we are at a crossroads with a unique opportunity to determine whether to offer consumers real control over their information or whether they should remain at the mercy of those doing the data collecting. CDT expects that the FTC will stand up for consumers and continue to bolster its role as one of the leading agencies in the world safeguarding consumer privacy.

This Commission has a great opportunity to make its mark on history by creating a strong framework in favor of privacy, and we urge the FTC to make the most of it.

---

[50] *See* Center for Democracy & Technology, Browser Privacy Features: A Work In Progress (Aug. 2009), *available at* www.cdt.org/privacy/20090804_browser_rpt_update.pdf.

[51] *See* Harbour Concurring Statement ("I encourage the technology community, including companies that develop browsers and software utilities, to focus their efforts on developing viable and transparent alternatives.").

[52] The FTC should join and follow Ann Cavoukian's commendable efforts here. *See* What is Privacy by Design?, http://www.privacybydesign.ca (last visited Nov. 5, 2009). The European Commission has also released several documents and held several workshops in support of developing FIPs.

[53] For example, see Pete Cashmore, *Privacy is dead, and social media hold smoking gun*, CNN, Oct. 28, 2009, http://edition.cnn.com/2009/OPINION/10/28/cashmore.online.privacy/ (last visited Nov. 5, 2009).

**Before the**

**FEDERAL COMMUNICATIONS COMMISSION**

**Washington, D.C. 20554**

| | | |
|---|---|---|
| In the Matter of | ) | |
| | ) | |
| A National Broadband Plan for our Future | ) | GN Docket Nos. 09-47, 09-51, 09-137 |
| Comments – NBP Public Notice #29 | ) | |
| | ) | |
| | ) | |

# COMMENTS OF THE CENTER FOR DEMOCRACY & TECHNOLOGY: APPENDIX B

## Applying Privacy by Design Principles to the Data Minimization FIP Principle and to Sensitive Data

## I. Using Privacy by Design to implement the Data Minimization FIP principle

Adherence to the Data Minimization FIP principle requires careful attention to the principles of Privacy by Design. The data minimization principle requires that attention is paid to end-to-end lifecycle protection of data; data practices must take into account which data will be collected, how long it will be retained, and in what form it will be stored. Below, we describe in greater detail the considerations that companies and government agencies that are handling individual-level data should remain aware of as they seek to implement the Data Minimization FIP principle in a manner consistent with Privacy by Design.

### A. Understanding data types

The Data Minimization principle requires that entities only collect data "that is directly relevant and necessary to accomplish the specified purpose(s) and only retain [that data] for as long as is necessary to fulfill the specified purpose(s)."[1] A determination of which data fulfills these criteria should hinge, in part, on the degree of data identifiability necessary to fulfill the specified purpose. If knowing that an individual user is a 20-year-old male is sufficient to the purpose at hand, then the data should be rendered pseudonymous, the user's name replaced with a unique ID. But if the goal is simply knowing the geographic breakdown of a site's visitors (what percent come from New York? What percent come from Kansas?), then no individual-level data needs to be maintained – aggregate statistics about users' location are sufficient.

---

[1] *See* 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* (Dec. 2008), *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf ("DHS FIPs").

Distinctions between data types have long been over-simplified, with vast quantities of data split into two supposedly distinguishable bins: one that holds "personally identifiable information" ("PII") and one that holds "non-personally identifiable information" ("non-PII"). PII has traditionally consisted of direct identifiers such as name or Social Security Number. Non-PII constitutes almost anything else. But the rules and the assumptions on which the distinction between PII and non-PII is constructed need to be reevaluated. Research has consistently shown that information can appear "de-identified" (and "anonymous") when alone, but when combined with other data, can help construct an identifying image of an individual. There have been a number of high profile examples of such re-identification. More then a decade ago, then-MIT graduate student Latanya Sweeney used Massachusetts residents' ZIP code, birth date, and gender - all found in public voter rolls - to identify individuals whose "anonymized" hospital records had been publicly released;[2] in 2006, AOL's infamous release of "de-identified" search terms led to the identification of individuals based on their search history. Meanwhile, researchers have shown that supposedly "anonymized" data released by Netflix was anything but anonymous.[3]

Recognition is finally growing in some quarters that information can identify an individual even absent the individual's name or Social Security number. In its 2008 staff report on online behavioral advertising, the FTC included within the scope of its behavioral advertising principles "any data collected for online behavioral advertising that reasonably could be associated with a particular consumer or computer or other device," regardless of whether the data is "personally identifiable" in the traditional sense.[4]

CDT believes this phrasing represents a significant change in the discourse. More broadly, collected data should be evaluated on a spectrum that ranges from identifiable data to pseudonymous data to aggregated data. Principles that guide data collection, protection, and use practices should appropriately reflect the pseudonymity of the data.

In 2009, CDT worked with companies and other advocacy organizations in our Internet Privacy Working Group (IPWG) to establish a workable and specific vocabulary to describe how data is stored and used online. Below, we present a set of definitions to measure data identifiablity that is based on IPWG's work.[5] We are confident that definitions like these can help move the discourse in a direction that is better aligned with reality and research. These definitions measure data identifiability from the perspective

---

[2] *See* Sweeney, Latanya *Recommendations to Identify and Combat Privacy Problems in the Commonwealth Before the H. Select Comm. on Information Security*, *Statement of Latanya Sweeney, Associate Professor, Carnegie Mellon University* (Oct. 2005) *available at* http://privacy.cs.cmu.edu/dataprivacy/talks/Flick-05-10.html

[3] *See e.g.* Arvind Narayanan & Vitaly Shmatikov, *Robust De-anonymization of Large Sparse Datasets*, IEEE Symposium on Security and Privacy (2008), *available at* http://www.cs.utexas.edu/~shmat/shmat_oak08netflix.pdf; Michael Barbaro & Tom Zeller, Jr., *A Face is Exposed for AOL Searcher No. 4417749*, N.Y. TIMES, Aug. 9, 2006, *available at* http://www.nytimes.com/2006/08/09/technology/09aol.html?_r=1&scp=1&sq=a%20face%20is%20exposed%20for%20AOL%20searcher&st=cse (AOL incident highlights the difficulties in making data truly anonymous).

[4] *See* Federal Trade Commission Staff Report, *Self-Regulatory Principles For Online Behavioral Advertising: Behavioral Advertising Tracking, Targeting & Technology* (Feb. 2009), *available at* http://www.ftc.gov/opa/2009/02/behavad.shtm.

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

of the entity collecting and using data for online advertising (as opposed to an outside observer or statistician, for example). How easy or hard it may be for such an entity to use data to identify an individual depends on the other data sources available to the entity, the capabilities of the entity, and the time, effort, and cost required to identify individuals. Note that all inferably identifiable data is pseudonymous, but all pseudonymous data is not necessary inferably identifiable.

- Aggregate data – Data about multiple individuals that cannot reasonably be used to directly or inferably identify any single individual.
- Directly identifiable data – Data that directly and overtly identifies an individual, such as name, address, email address, phone number, government identifier, or financial identifier.
- Inferably identifiable data – Data from which an individual's identity can be reasonably inferred, including combinations of data elements or data sets that would not, on their own, identify an individual. All inferably identifiable data is pseudonymous.
- Pseudonymous data – Data associated with a unique identifier that does not directly identify an individual.

### 1. "Aggregate" data

Information about an individual that has been aggregated with information about others is often difficult, if not impossible, to re-associate with that individual. But if this aggregate data, known as tabular data, is subdivided into a sufficient number of categories and contains information about a small enough number of people, then information about specific individuals could reasonably be parsed out of the data set. A number of publications have detailed best practices for ensuring that individual information within tabular data is sufficiently protected, and they should be used as guidance for those who compile tabular data. In their 2008 statement entitled "Data Access and Personal Privacy: Appropriate Methods of Disclosure Control, the American Statistical Association recommends a subset of these guidelines."[6] Of these, a 2005 paper by the Federal Committee on Statistical Methodology (OMB) stands out. This paper lays out appropriate tests for determining if individuals whose information is stored in tabular data are at high risk of being identified and describes methods for managing and merging data such that data quality is preserved and privacy is better protected.[7]

---

[6] *See* American Statistical Association, *Data Access and Personal Privacy: Appropriate Methods for Disclosure: A Statement by the American Statistical Association* (Dec. 6, 2008). *available at* http://www.amstat.org/news/statementondataaccess.cfm.

[7] *See* Federal Committee on Statistical Methodology, *Statistical Policy Working Paper 22 – Report on Statistical Disclosure Limitation Methodology* (2005), *available at* http://www.fcsm.gov/working-papers/spwp22.html

### B. Principles to guide data minimization

The collection of large amounts of individual-level data and the accumulation of this data in directly identifiable or pseudonymous form long after it is no longer useful presents some of the greatest privacy risks for consumers.

As mentioned above, in 2009, CDT submitted comments to the OMB on their proposed revision to the federal policy on Web tracking technologies. In these comments, we outlined a set of Data Minimization principles that should guide federal agencies that collect individual-level data for measurement purposes.[8] We have updated these principles to make them applicable to corporate entities that collect individual-level data for measurement purposes as well as for those who collect this data for other purposes.

Entities collecting individual-level data and their commercial partners should take the following steps in connection with limiting data retention:

- **Purpose correlation.** *Only data directly relevant and necessary to accomplish a specified purpose should be collected and individual-level data should only be retained for as long as is necessary to fulfill a specified purpose.*

- **Immediate deletion.** *Elements of individual-level data logs that are not relevant to the analyses proposed in the manner specified by the Purpose Specification FIP principle should be deleted as soon as possible after the data is collected. If, for example, the entity has promised to pseudonymize data, IP addresses should be deleted (and possibly replaced with their corresponding geographic or ISP information) soon after collection, if not immediately.*

- **Disclosure**. *Data retention time frames should be published in privacy policies.*

- **Technical enforcement.** *Expiration time frames for cookies and other technologies that store data on users' computers should be set to match, not exceed, the data retention time frames adopted by the entities who place the cookies.*

- **Partner contracts.** *If an entity contracts with a commercial partner who will collect measurement data, place cookies, or otherwise collect or store individual-level information, the data retention time frames that apply to individual-level data collected by the partner should be explicitly stated in the contract.*

---

[8] *See* Center for Democracy & Technology, *Comments Regarding the Office of Management and Budget's Proposed Revision of the Policy on Web Tracking Technologies for Federal Web Sites* (August 2009), *available at* http://www.cdt.org/privacy/20090810_omb_cookies.pdf.

Using these principles to guide implementation of the Data Minimization FIP principle will promote consumer privacy in a manner that does not interfere with innovation.[9]

## II. Applying Privacy by Design to sensitive data

The services made possible by broadband Internet create and collect a wide range of data and much of it can be extraordinarily sensitive in nature. For example, people tell search engines things they would not tell their friends, spouses, or therapists. They store information about their diet, exercise, medicines, and illnesses in Personal Health Records, information they might not tell their bosses or insurance companies. Meanwhile, banking, mortgage, and tax information is increasingly shared with cloud-based applications, while smart phones serve as accurate tracking devices – crumbs of zeroes and ones mark exactly which stores, offices, and residences each customer visits, data that third-party applications are all too eager to mine.[10]

CDT believes that the collection and use of sensitive data by companies operating in the online space necessitates an extra level of protection; it is imperative that companies that plan to collect or use sensitive data pay particularly close attention to the Privacy by Design principles, and use these principles to guide their implementation of FIPs. This is especially important with respect to location information, a relatively new and rapidly expanding data type that promises great benefits, but also incurs substantial privacy risks, for consumers.

As Congress and federal agencies work to establish rules for managing information collected online and deliberate about what extra protections certain information deserves, they will need a precise definition for the term "sensitive data." We believe that the term "sensitive data" should be defined, at a minimum, to include:

---

[9] The data retention elements outlined in this set of principles would represent an improvement over the FTC's current data retention principle, at least in the online behavioral advertising space. With respect to online behavioral advertising, the FTC only recommends that "companies should retain data only as long as is necessary to fulfill a legitimate business or law enforcement need." This is inadequate. The FTC's version of the principle does not guard against unanticipated uses because data retention is not tied to the purpose for which the data was collected in the first place. *See* Federal Trade Commission Staff Report, *Self-Regulatory Principles For Online Behavioral Advertising: Behavioral Advertising Tracking, Targeting & Technology* (Feb. 2009) at 47, *available at* http://www.ftc.gov/opa/2009/02/behavad.shtm.

Indeed, it is not the FTC but a company that recently pushed the market toward a higher standard for data retention. Yahoo! recently made changes to its data retention policy so that the company now removes directly identifiable data and some inferably identifiable user log data after three months. Yahoo's decision was based on its determination that the purpose for which the data was initially collected would not be served by data more than three months old. Three months might be a suitable retention limit for some data; the research showing that the data most relevant for marketing purposes is a mere 24 hours suggests that shorter periods may be appropriate for marketing data. Since Yahoo's announcement, Microsoft has also announced that it will reduce the amount of time that it stores IP addresses. *See e.g.,* Walaika Haskins, *Yahoo Pledges to Forget You Sooner*, TECHNEWSWORLD (Dec. 17, 2008), *available at* http://www.technewsworld.com/story/65545.html?wlc=1255717445; Kevin J. Obrien, *Microsoft Puts a Time Limit on Bing Data,* New York Times (January 19, 2010), *available at http://www.nytimes.com/2010/01/20/technology/companies/20search.htm.*

[10] Often, these applications use location data for the benefit of consumers. *See, e.g.,* Google Latitutde *available at* www.google.com/latitude; Loopt, *available at* www.loopt.com.

- Information about past, present, or potential future health or medical conditions or treatments, including genetic, genomic, and family medical history information of an individual;
- Financial information about an individual;
- Information about an individual's sexual behavior or sexual orientation;
- Social Security Numbers or any other government-issued identifiers;
- Insurance plan numbers;
- Information indicating the precise geographic location of an individual when he or she accesses the Internet.[11]

### A. Location Information and the Dawn of the Location Enabled Web

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 that have not yet been adequately addressed.

#### 1. Definitions to guide discussions of location Information

The IPWG Threshold Analysis also establishes workable and specific definitions for the types of location information that are commonly created and collected online. The location definitions are based on terminology used by technical standards bodies that focus on location information and privacy, most notably the Internet Engineering Task Force (IETF) Geographic Location/Privacy Working Group.

> Civic location data – Data that describes the geographic location of an individual in terms of a postal address or civic landmark. Examples of such data are room number, street number, street name, city, ZIP+4, ZIP, county, state, and country. The precision of this data can be reduced by removing elements (for example, the precision of the combination of city, state and ZIP can be reduced by only using state).
>
> Geodetic location data – Data that describes the geographic location of an individual in a particular coordinate system (for example, a latitude-longitude pair). The precision of this data can be reduced by specifying a geographic area of particular spectrums rather than a point (for example, a circle with a 300 meter radius centered at 40° North, 105° West). However, the limits of such a precision

[11] Both in the following section and in CDT's 2009 Threshold Analysis for Online Advertising Practices, we subdivide location data into five categories: civic location data, geodetic location data, mobile location data, fixed location data, and nomadic location data. We believe that all mobile location data, fixed location data, and nomadic location data is sensitive in nature. Geodetic location data and civic location data can be sensitive depending on the precision o the data. Center for Democracy & Technology, *Threshold Analysis for Online Advertising Practices* 16 (Jan. 2009), *available at* http://www.cdt.org/privacy/20090128threshold.pdf.

specification can be circumvented by repeatedly sampling an individual's geodetic location.

Mobile location data – Civic or geodetic location data that identifies the whereabouts of an individual or his or her device in real or near-real time.

Fixed location data – Civic or geodetic location data that describes a fixed location associated with an individual. Examples include a home or office location.

Nomadic location data – Civic or geodetic location data that identifies the whereabouts of an individual using a device that may be moved occasionally from its fixed location. For example, if an individual occasionally uses his or her laptop at an Internet cafe, the location of the laptop would be considered nomadic.

### 2. Special considerations for sensitive location information

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 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.[12]

But in terms of providing more granular control and transparency, the browsers are lacking. 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,

---

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

much like the “lock” icons that indicate a secure connection, an icon could be displayed on the browser whenever Safari is transmitting location data. A similar regime for location data could encourage good practices from application providers.

**Before the**

**FEDERAL COMMUNICATIONS COMMISSION**

**Washington, D.C. 20554**

| | | |
|---|---|---|
| In the Matter of | ) | |
| | ) | |
| A National Broadband Plan for our Future | ) | GN Docket Nos. 09-47, 09-51, 09-137 |
| Comments – NBP Public Notice #29 | ) | |
| | ) | |
| | ) | |

**COMMENTS OF THE CENTER FOR DEMOCRACY & TECHNOLOGY: APPENDIX C**

**Looking Back at P3P: Lessons for the Future, a paper by Ari Schwartz, Vice President and COO of the Center for Democracy & Technology, November 2009**

## I. Introduction

A number of people who work on data protection have begun examining the idea of machine-readable statements that can express the privacy practices of a Web site or a third-party intermediary, such as a network advertiser or an analytics company.[1] The theory is that such statements would provide a clear, standardized means of rendering potentially complex privacy policies into a format that could be automatically parsed and instantly acted upon.

The idea is a good one. It harnesses the power of information technology to create a means for transparency and user choice. However, it is hard to overlook the fact that there is already a Web standard to do precisely the same thing, and it hasn't been very successful.

The Platform for Privacy Preferences (P3P) is a standard of the World Wide Web Consortium (W3C), the main standard setting body for the Web. P3P has never been fully implemented as its creators had hoped. While it is in use today and functions in some ways as we thought it might, P3P is unlikely to be broadly adopted or to accomplish all that those pushing for machine-readable policies would like.

This is not meant to suggest that using P3P is passé; or that creating new machine-readable standards based on P3P is a waste of time; or that creating interfaces that could be used for machine-readable policies is a fruitless exercise. In fact, the opposite

[1] Ideas on machine-readable policies have been discussed at recent conferences such as the Privacy Bar Camp DC; the NYU privacy legislation symposium; the Engaging Data Forum at MIT and other events that I've attended. As recently as Winter 2009, companies have come to discuss this with the Center for Democracy and Technology (CDT) as if it were a completely new idea.

is true. Machine-readable policies, like other PETs, hold considerable promise and deserve attention. However, to create machine-readable policies that work, we need to learn from how P3P was created and promoted, study its shortcomings, and draw from the immense amount of effort put into the project, where possible.

I worked actively on the P3P standard process and helped to promote its deployment from 1998 – 2003. During that time, we ran into many obstacles as we sought full-scale P3P implementation. This paper is meant to summarize the issues involved and my recommendations (political, economic and ethical) for those who would like to build and promote machine-readable privacy standards in the future.

## II. History

P3P has a long and complex history detailed by Carnegie Mellon Professor Lorrie Cranor in her book on privacy and P3P.[2] I will refrain from repeating this story and instead only focus on parts that are relevant to understanding the hurdles and achievements with P3P.

The theory behind P3P can be traced back to the mid-1990s. Many have claimed credit for the idea of using machine-readable policies for variety of different social purposes. This was just before the birth of XML and there was a realization that metadata would be useful for different purposes but few ideas how to make it a success in a public policy framework. As the privacy debate, in the United States and elsewhere, began to focus on encouraging companies to post human-readable privacy policies and as criticism increased about the complexity of those notices, there was a call to simplify them through standardization. If policies could be narrowed down to the equivalent of a multiple-choice set of options, then they could be made machine-readable.

After discussions about this theory at the Internet Privacy Working Group,[3] the idea of P3P was passed to the main standards setting body for the Web, the World Wide Web Consortium (W3C). The W3C was charged with creating a P3P working group that would create the technical standards, the vocabulary, and the data schemas that would be used to make up the multiple choice questions. The W3C started its work on P3P in 1997 and the P3P Specification Working Group was chartered in July 1999.[4]

### 1. Building and Over-Building

Early on, as it became apparent that there were disparate views within the P3P Specification Working Group, it was decided that a set of "Guiding Principles" should be adopted to structure and inform future work. The principles adopted were as follows:

- *Information Privacy*

---

[2] Lorrie Cranor, Web Privacy with P3P, O'Reilly, Sebastopol, CA, 2002.

[3] The Internet Privacy Working Group (IPWG) is a forum of public interest groups, companies and academics convened by the Center for Democracy and Technology (CDT).

[4] The P3P site has a history of all versions of the specification — http://www.w3.org/p3p.

    - *Service providers should preserve trust and protect privacy by applying relevant laws and principles of data protection and privacy to their information practices.*
    - *Including:*
    - *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data*
    - *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data of 1980*
    - *US HEW Fair Information Principles of 1971*
- *Notice and Communication*
    - *Service providers should provide timely and effective notices of their information practices, and user agents should provide effective tools for users to access these notices and make decisions based on them.*
- *Choice and Control*
    - *Users should be given the ability to make meaningful choices about the collection, use, and disclosure of personal information. Users should retain control over their personal information and decide the conditions under which they will share it.*
- *Fairness and Integrity*
    - *Service providers should treat users and their personal information with fairness and integrity.*
- *Security*
    - *While P3P itself does not include security mechanisms, it is intended to be used in conjunction with security tools. Users' personal information should always be protected with reasonable security safeguards in keeping with the sensitivity of the information.*[5]

These principles helped resolve questions that arose about the intent of the standard.

Despite having this road map, the P3P specification changed dramatically over time. Pieces were added and then taken away. Professor Cranor has aptly compared the process to out-of-control construction on a kitchen that at first only needs a small new appliance (a toaster) but ends up with a plan for new cabinets, floors and lighting. Controversial ideas for negotiation, automated data transfer and others were added. Fortunately, discussions about the complications introduced by these additions — as well as the significant work required just to finish the vocabulary alone — led the group to cut back on all of these ideas and to more or less return to the original plan. However, a lot of time and effort was wasted debating these large-scale additions to the specification.

### A. Caught Up in the Politics of Privacy

P3P had many critics when it was first created. At first, most of the concern came from some influential privacy advocates who believed that P3P was merely a ruse to stop greater regulation of the online industry. Later, concern came from traditional industry

[5] http://www.w3.org/TR/NOTE-P3P10-principles.

members that either did not want to have to implement P3P or that saw P3P was too transparent and therefore a threat to existing business models that consumers would disapprove of once they realized how their information was being used.

### 1. Criticized by some privacy advocates as an industry subterfuge

Early in its development, critics of P3P raised concerns that the standard was intended to stave off consumer privacy legislation in the United States and to allow companies to evade current law in the European Union.

The early decision to tie an automated data transfer standard, know as the Open Profiling System (OPS), to P3P was particular damaging. A preliminary assessment from the Article 29 Working Party in the EU, written in July 1998 before the Specification Group was even formed, raised concerns about several issues including a fear that OPS would be used to negotiate away privacy protections girded by law.[6]

The legitimate concern that companies would use OPS to limit user choice was raised again and again, even after OPS was completely removed from the specification. When P3P was defended as merely one piece of a broader set of solutions in technology and law, many critics were still concerned. As librarian and activist Karen Coyle said in 1999: "Many people will not understand that 'privacy practices' are not the same as 'privacy.' P3P therefore allows sites to create an air of privacy while they gather personal data."[7]

CDT worked with the Ontario Privacy Commissioner, Ann Cavoukian, and her staff to lay out the reasons why, once OPS was removed, a correctly implemented P3P actually could strengthen privacy. In 2000, we published a paper[8] plainly stating that P3P was not a panacea for privacy. We emphasized that neither P3P nor any other privacy enhancing technology (PET) can solve all privacy issues. Instead, we argued, P3P needs to be used in concert with effective legislation, policy oversight and other privacy enhancing tools. We spelled out four ways in which P3P could help protect privacy:

> 1. *Countries with data protection and privacy laws and others seeking to police compliance with privacy standards could find the automated ability to assess a businesses' privacy statement useful in their broader oversight and compliance program* – Searching and gathering privacy policies could be simplified through P3P as P3P would allow these policies to be collected and analyzed in a standard machine-readable format. Governments and organizations would be able to simply search through P3P statements to find companies whose notice does not meet privacy standards in various areas. In the current version of P3P, companies could even point to regulatory bodies that oversee them to help route privacy complaints.

---

[6] http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/1998/wp11_en.pdf.

[7] Karen Coyle, "P3P: Pretty Poor Privacy?" http://www.kcoyle.net/p3p.html.

[8] P3P and Privacy: An Update for the Privacy Community, Ann Cavoukian, Mike Gurski, Deirdre Mulligan and Ari Schwartz, March 28, 2000 http://www.cdt.org/privacy/pet/p3pprivacy.shtml.

2. *Users could more easily read privacy statements before entering Web sites* – Privacy notices are frequently written in complicated legalese. P3P implementations could allow users to assess privacy statements prior to visiting a site, and allow users to screen and search for sites that offer certain privacy protections.

3. *P3P could cut through the legalese* – A company's P3P statement cannot use difficult to understand or unclear language. The standardization and simplification of privacy assertions into statements simple enough to be automated will allow users to have a clear sense of who does what with their information.

4. *Enterprising companies or individuals could develop more accurate means of rating and blocking sites that do not meet certain privacy standards or allow individuals to set these standards for themselves* – Creating the tools and knowledge that support products to rate and vet Web sites is difficult and time consuming. By providing an open standard, P3P could enhance the transparency, accuracy and detail of existing products, and could encourage an influx of new privacy enhancing products and services.

### 2. Cited by some industry advocates as a substitute for legislation

Unfortunately, several libertarian commentators and US politicians – even though they were not working on the specification— actively promoted P3P as a stand-alone solution, thereby reviving the concerns that CDT and the Ontario Privacy Commissioner had attempted to dispel. For example, in testimony before the Senate, the chairman of the US Federal Trade Commission (FTC) cited a Progress and Freedom Foundation report that suggested that 23 percent of Web sites had implemented P3P as a reason not to implement privacy legislation.[9] The chairman neglected to mention that the report did not look into whether the P3P policies were compliant with the P3P standard, which many were not, and did not assess whether the policies actually offered privacy protections commensurate with either the European Data Protection Directive or the proposed standard in the bill that he was arguing against.

It is interesting to compare this reaction to that of the European officials who looked at P3P at the same time and correctly saw both its value and its limitations:

> Among European Privacy Protection Commissioners the consensus grows: P3P is useful for online privacy, but not sufficient on its own because P3P offers only a basic standard for privacy protection. Under any circumstances, additional effective privacy monitoring and precise laws to protect Internet users are required.[10]

### 3. Criticized by some in industry for providing consumers too much transparency

---

[9] Statement for the record of FTC Chairman Timothy Muris, S. Hrg. 107-1150, Hearing before the Senate Energy and Commerce Committee on S. 2201, the Online Personal Privacy Act, April 25, 2002. p. 11.

[10] Independent Centre for Privacy Protection Schleswig-Holstein, Press Release on P3P, August 29, 2000 – http://www.datenschutzzentrum.de/somak/somak00/p3pe_pm.htm.

After the Specification Group started its work, many companies became increasingly concerned that P3P would empower users with too complete an understanding of how they were being tracked by companies. Most of these companies would only discuss these ideas behind closed doors, but at least one of the companies' analyses was made public.

Two Citibank employees published a paper expressing "concern that P3P would let ordinary users see, in full gory detail, how their personal information might be misused by less trusted or responsible web site operators."[11] This criticism from industry came up frequently in the P3P Working Groups. While a majority of the Working Group remained committed to the guiding principle of transparency, different companies ended up making different choices about how much they really wanted to be transparent with consumers. Two examples:

- A number of company argued that instead of only offering binary responses within the categories for types and uses of data, P3P should contain 3 options — Yes (we collect this data), No (we do not collect this data), Maybe (we may collect this data). The majority of the group felt strongly the binary yes/no option was important for transparency and that "Maybe" had to be treated as a "Yes" to be understood by consumers. One company, which had spent dozens of hours and thousands of dollars following the P3P process, was extremely insistent on this point and, in the end, never implemented P3P.[12]

- When P3P was finally implemented, a company that had worked on the specification complained, behind closed doors, that implementing the full specification would make them look bad and could stop users from accessing some of their sites. After realizing that implementing only part of the specification might leave them open to a charge of deceptive practices in the US and Europe, the company did implement a policy that was compliant with the specification.

There have also been many positive stories about companies that instituted new privacy-friendly policies when confronted with having to implement P3P. The transparency that P3P offers clearly had an impact on companies when they confronted the realization that P3P would make their privacy policies much more public.

### B. Web sites build to the implementation, not the specification

Throughout 1998 and 1999, there was a lot of discussion about whether P3P had a "chicken and egg" problem. The concern was that P3P policies wouldn't be created until

---

[11] Kenneth Lee and Gabriel Speyer, "White Paper: Platform for Privacy Preferences Project (P3P) and Citibank" http://www.w3.org/P3P/Lee_Speyer.html.

[12] This point is reflected in early public comments from BITS, The Technology Group for The Financial Services Roundtable available at http://www.w3.org/2002/p3p-ws/pp/bits.pdf. And more strongly at http://www.bitsinfo.org/downloads/Comment%20letters/W3CCommentLetter.pdf —where BITS made clear that their specific goal was to try to make P3P statements as confusing as written statements are on the Web: "[O]ne of the most significant decisions of the P3P Working Group was not to enable use of the word "may" within the P3P nomenclature. We believe that the P3P nomenclature should enable verbatim translation of existing plain language policies, and that failure to incorporate that capability will materially affect the speed with which this standard is adopted in the marketplace."

there was implementation in a widely used consumer product such as a Web browser, but the browser implementation wouldn't do anything until there were policies online. There was an effort to get many sites compliant, but until consumer products existed those efforts were not very successful.

In October 2000, after the second working draft of the P3P specification was released, several consumer products were created. Most notably, Microsoft built P3P capabilities into Internet Explorer 6. However, those features mostly focused on utilizing an optional part of the P3P specification called the "compact policy." The compact policy takes all of the categories of information and all of the purposes for which they were used and ties them together, losing much of the subtlety that P3P full policies promised, but gaining an ability to read the policies more quickly. Internet Explorer 6 also put the strongest defaults on the use of "third-party cookies," a term that is not even in the P3P specification. Microsoft decided not to utilize the main source of metadata — the full P3P policy as opposed to the compact policy —from P3P policies to help consumers control the release of their personal information based on what is actually happening to that data rather than an abstract summary offered by the compact policy. Because of these decisions, the P3P compact policies are in widespread use among companies that place third-party cookies demonstrating the power of a single implementation in the browser.

Unfortunately, there are still no good tools that make use of the metadata and this is why the main portion of the P3P specification is only used by a minority of Web sites today.

## III. Recommendations for the Future

When thought of as an important experiment in categorizing privacy practices, P3P has been a qualified success. On the other hand, if the goal of P3P was either to protect the privacy of users on its own or, for the Internet industry, to stave of the threat of regulation, P3P should be viewed an abject failure.

However, as a standard that works in conjunction with "additional effective privacy monitoring and precise laws to protect Internet users" (as the Independent Centre for Privacy Protection Schleswig-Holstein) current P3P implementations are a minor success and an indicator of what can still be accomplished with machine-readable polices.

Also, as a case study in the pitfalls and potentials of efforts to develop PETs, P3P is undeniably valuable. As new metadata standards for privacy are created based on P3P and as other PETs are explored, there are several lessons to learn from the P3P project experience:

### A. Keep it simple

P3P is far too complex as it stands today.

For example, the standard includes 17 categories for data-type and 12 categories for data-use that Web sites can include in their meta-data; four of the data-use categories cover different types of profiling. There are many legitimate reasons that these

categories exist,[13] but the sheer number leads to far too many combinations and is overwhelming both for programmers and for Webmasters who would otherwise be interested in implementing P3P. Compliance is not difficult for a Web site with a clear and simple privacy policy, but many companies just aren't wiling to put in the effort to understand all of the categories and purposes.[14]

In their book *Nudge: Improving Decisions about Health, Wealth and Happiness*,[15] Richard Thaler and Cass Sunstein discuss the problems created by overwhelming choice and how to create workable options for individuals in policy and technology. Anyone interested in creating the next round of metadata technologies must read *Nudge* and consider how its recommendations on setting options and defaults would work in the particular context. My reading is that there should be no more than four options and the default should be set higher than average practices on the Internet today.

### B. There is no "chicken and egg" problem: build the interface to use metadata first

Too much time and effort was spent trying to convince Web site operators of the value of implementing P3P on their Web sites. Either the market will work or direct regulation will dictate the value for the companies, or the idea will fail, but in no case is it possible for the developers of a concept like P3P to create critical mass of acceptance among Web sites – there are simply too many Web sites to convince to gain that critical mass. The evidence from the relatively successful implementation of P3P for cookies in Internet Explorer demonstrates the value of working with browser makers or with developers in other spaces that have ready access to direct user interfaces (as opposed to add-on tools) to implement solutions that utilize the metadata in ways that clearly benefit consumers. After these solutions are in place, companies will be forced to implement by the economics of having sites blocked or tagged.

### C. Manage expectations: companies shouldn't use a metadata solution to argue for less regulation

If you are looking for a way to prevent over-burdensome privacy legislation or regulation and you believe that metadata tools are a means to accomplish this, you need to think again. Too many companies and trade associations spent more time arguing for the benefits of P3P in Washington and Brussels and too few spent effort building P3P into products. Perhaps at some point, widespread and effective use of metadata tools will justify a loosening of regulatory requirements, but even after adoption is completely ubiquitous, we would need testing and facts to prove that the technology was in fact

---

[13] In one telling example, when the White House was implementing P3P, officials there found that the specification did not have an option allowing them to express that they were required by law to store information for historical purposes. It was decided that many governments would have this same issue, so a "historical" purpose was added.

[14] Professor Cranor suggests that both categories should be cut down to eight, which would be more manageable for programmers, but would still need to be cut down further by the programmers to be successful. She and her students use P3P policies to automatically generate a privacy "nutrition label" in the form of a table with 10 rows and 6 columns. This format hides some of the complexity of P3P by representing multiple P3P elements in a single row or column. http://cups.cs.cmu.edu/privacyLabel/

[15] Richard Thaler and Cass Sunstein, Nudge: Improving Decisions about Health, Wealth and Happiness, Penguin, 2009.

effective. And of course, it would be just as easy to add metadata requirements into regulations for transparency as it would be to use them to prevent regulation. In fact, it would be a particularly inexpensive addition compared to the rest of the cost of data protection legislation. I am not advocating this approach as a solution as much as I am trying to point out that the development of PETs and the debates over regulation should take place on largely separate tracks, with participants checking in only to ensure that new regulations match the vocabulary in the metadata. Neither the development of PETs nor the regulatory debate will be well-served by those who engage in the PETs development process mainly to bolster their arguments against legislation.

### D. Learn from the work that has been done on P3P

Finally, a lot of good work went into P3P. It is not a dead standard. Those who use third-party cookies regularly are implementing it now more than ever. However, it can be improved and it will need to be modernized in order to reach the original vision where the metadata of the full policy is parsed and used regularly. This could mean revamping P3P or it could mean developing something new. In any case, starting from scratch will only mean running into some of the same hurdles faced by the W3C P3P working groups. The history and work of P3P should be a launching place, not something to throw aside.

**Before the**
**FEDERAL COMMUNICATIONS COMMISSION**
**Washington, D.C. 20554**

| | | |
|---|---|---|
| In the Matter of | ) | |
| | ) | |
| A National Broadband Plan for our Future | ) | GN Docket Nos. 09-47, 09-51, 09-137 |
| Comments – NBP Public Notice #29 | ) | |
| | ) | |
| | ) | |

**COMMENTS OF THE CENTER FOR DEMOCRACY & TECHNOLOGY: APPENDIX D**

**PRIVACY PRINCIPLES FOR IDENTITY IN THE DIGITAL AGE, Draft for Comment - Version 1.4, December 2007**

## I. INTRODUCTION

### Intersection of Identity and Technology

How to create and manage individual identity is becoming a central challenge of the digital age. Various identity-related initiatives are being developed and implemented in both the public and private sectors. A major goal of many of these programs is to prevent illegal activity or enhance security, whether it be the security of our national borders, airplanes, workplaces, health records, or online transactions. Identity-related technologies – such as databases, machine-readable identification cards, and online accounts – can help realize the potential of the digital age, whether by making e- commerce exchanges more seamless, tying together information on multiple devices, combating fraud, or enabling yet unimagined services. Increasingly, as individuals go about their lives online and off, they will be generating or disclosing personal information or will be asked to identify themselves in some way. Undoubtedly, the range of transactions and events that can be linked to individual identity will grow.

However, the collection, storage, and disclosure of identity information can create risks to personal privacy and security. Poorly implemented identity systems can unnecessarily invade the privacy of innocent Americans, and can actually contribute to identity theft or weaken security. The digitization of information – by facilitating the collection, storage and sharing of large amounts of data – can exacerbate the privacy and security risks inherent in identity systems.

To mitigate these risks while achieving the benefits of identity systems, it is essential that these systems be designed with effective privacy and security measures built in. Incorporating such protections at the very beginning will help achieve the goals of identity systems while maximizing user control and other elements of privacy.

### Summary of the Principles

In this document CDT outlines the following 11 privacy and security principles to guide public and private sector entities in the development of programs or systems involving the collection, authentication, and use of identity information:

| Overarching Principles | Principles Based on FIPs |
|---|---|
| • Diversity & Decentralization<br>• Proportionality<br>• Privacy & Security By Design | • Purpose Specification<br>• Limited Use<br>• Notice<br>• Individual Control and Choice<br>• Security<br>• Accountability<br>• Access<br>• Data Quality |

The first three principles are overarching guidelines that are particularly relevant to identity in the digital age. The remaining eight principles are adaptations of the widely recognized fair information practices (FIPs) to the identity context.

The principles focus on privacy but also address security in certain instances. This is because privacy and security are interrelated and often should be considered together. When privacy is compromised, security of the individual, the organization or even the country is also threatened. Conversely, security breaches can also lead to invasions of privacy.

This document is meant to apply only to systems that identify individuals rather than groups or other entities.

The remainder of this section provides a general framework for understanding these principles. Section II discusses the principles themselves. Section III contains a glossary of terms used throughout this document.

**Are privacy and identification at odds with each other?**

For those with limited exposure to the concepts of identity and privacy, it may seem as though identification and privacy are in contradiction to each other. In many cases, this is true: privacy can be served though the lack of identity. Anonymity is a constitutional right in some circumstances. As individuals are increasingly required to reveal more information about themselves and authenticate their identities more often, their privacy may be at greater risk.

However, the relationship between identity and privacy is a nuanced one. Consider a fraud detection system as an example. To determine if a particular transaction involves the fraudulent use of identity – and if an innocent individual's financial or other personal information has been compromised – it is useful to gather a good deal of information about the transaction and the identity claims of the individual seeking to engage in the transaction. This information can be compared with other identity information that has been compiled for fraud prevention purposes. Although gathering a lot of identity information may seem antithetical to privacy interests, in this case it may actually help to protect privacy by identifying an instance of identity theft. Thus, although in many cases less identification can mean more privacy, in this case the opposite may be true. Nevertheless, even an anti-fraud identity verification system can be designed in a pro-privacy fashion and should be guided by the principles set forth here.

The "less identification equals more privacy" idea also fails to take into account the type and sensitivity of the identity information involved. For example, a person's name, address, and

telephone number may constitute a greater quantity of information than the person's fingerprint or DNA profile, but the latter reveal much more about the person. Likewise, a small amount of identity information that is shared with a multitude of parties or is not properly secured may put an individual's privacy at greater risk than a large amount of information that is properly secured and accessed only by authorized parties.

These nuances ultimately lead to the conclusion that the evaluation of identity systems with respect to privacy must be done in context. Determining how to apply the principles set forth in the next section to a particular identity system will require a solid understanding of the environment in which the system operates and of all the risks and benefits that the system must balance.

**Goals of the Principles**

The purpose of this document is:

- To provide the public interest and privacy advocacy community with a general, high-level framework for evaluating the privacy and security of identity systems, and
- To provide policymakers, and identity system designers, implementers, and users – including those who may be unfamiliar with privacy concepts – with guidance on how to safeguard personal privacy and security in identity systems.

The ultimate goal of the principles is to help ensure that any given identity system maximizes personal privacy and security, or at the very least, minimizes invasions of privacy and threats to security. It should be noted, however, that applying all of the principles will not necessarily guarantee that a given identity system will be privacy- protective.. Nor are the principles intended to be a mere checklist. Rather, they are intended to spur the development of creative solutions.

The principles are interrelated and must be viewed as one overarching policy framework. All of the principles should be considered together when developing an identity system. However, while it is possible to apply each principle to an identity system, it may be that not all of the principles will apply to a given identity system with equal force. Policymakers and system designers must fully consider each principle and how it can be maximized within a given identity system, but may reasonably conclude that it is more appropriate or feasible to focus on some principles over others depending on the particular context or specified purpose of the identity system.

**Next Steps**

This Version 1.4 is a draft document that is open for comment. CDT continues to convene stakeholders with diverse perspectives on this issue with the hope of achieving a comprehensive set of guidelines that can be useful across the public and private sectors and in many different contexts.

## II. PRINCIPLES

### Preliminary Question: Is Individual Identification Necessary?

The first consideration for both governmental and commercial entities should always be whether an identity system is in fact necessary and effective for solving the problem at hand. Many goals can be accomplished without using any identity information at all.

Policymakers and system designers should not assume that adding an identification element to a system – an access system, payment system, communications system, or other transactional system – will make it more robust. The advantages of collecting and using identity, authentication, and linked information should be weighed against the risks to privacy and security.

Once a specific problem or goal is clearly articulated, the key question must be asked: Is individual identification necessary for solving the problem or accomplishing the goal? Developers should always be open to solutions that do not involve individual identification. However, if the answer is "yes," then the following 11 principles should be addressed during the development of the identity system.

Each principle below begins with a concise statement (in bold). A lengthier description and examples follow this statement.

### Overarching Principles

The first three principles are overarching guidelines that are particularly relevant to identity in the digital age.

#### ✦ Diversity and Decentralization

---

**Rather than attempt to serve as a perfect single solution, enrollment and authentication options should function like keys on a key ring, with different identities for different purposes. They should allow individuals to choose the appropriate option to satisfy a specific need. On balance, it is not optimal to centralize identity information or use a single credential for a multitude of purposes. In cases where linking of identity systems and databases is deemed necessary, appropriate safeguards should be implemented to limit the associated privacy and security risks.**

Using only one or a very small handful of centralized identity solutions for multiple purposes leaves individuals with few choices and diminishes the ability of identity systems to protect privacy and security. Requiring individuals to use a single identifier or credential for multiple purposes creates a single target for privacy and security abuses by identity thieves, terrorists, government, business, and others.

Using a single identity for multiple purposes may, however, offer convenience and efficiency benefits. These benefits should be weighed against the risk of concentrating identity information in a single location or credential.

EXAMPLE 1: Credit Cards

Individuals have the option of using merchant-specific credit cards or a single general- purpose credit card. Carrying a single card may be more convenient because it can be used in many different locations. However, this allows a single credit card company to maintain an individual's entire transaction history. Using multiple merchant-specific cards spreads this information among several parties.

It is important for both kinds of credit cards to exist so that individuals can weigh each option's benefits and drawbacks related to both privacy and convenience. Some may prefer the convenience of a single card, while others may prefer maintaining multiple separate transaction histories. Rather than requiring individuals to use one system or the other, both systems should be able to coexist.

Different government agencies, companies and organizations, and different types of functions within organizations, will likely need different types of identity systems. Identity systems should be designed to function in a marketplace offering multiple services that deliver varying degrees and kinds of enrollment, authentication, and use of identity information. This diversity of systems compliments the principle of Individual Control and Choice, which recommends that individuals be provided with options for expressing and authenticating their identities within a single system.

EXAMPLE 2: Diversity in Authentication Mechanisms

Consider the authentication mechanisms necessary for two different scenarios: accessing health records at a doctor's office, and accessing a Web-based email account.

At the doctor's office, a patient may be required to provide an identification card, such as a health insurance card, in order to access his or her own health records. The card might include information such as the patient's name and date of birth. Or a doctor or nurse may simply recognize a long-time patient and provide access to the appropriate records.

For Web-based email, a username and password combination is frequently used to authenticate the owner of an account. Some accounts may use two-factor authentication that combines knowledge of a password or PIN with possession of a security token or card. These authenticators may or may not reveal the account owner's name or other identity information.

Each of these authentication mechanisms is suitable to its own context. It would make little sense and may be harmful to privacy if individuals were required to login to their email accounts using a health insurance card – it is not necessary for most Web-based email providers to know the information on the card, and most cards are not remotely readable. Having a diversity of authentication mechanisms available is key to ensuring that suitable solutions exist for all kinds of authentication contexts.

The concept of decentralized storage and access to identity information closely parallels the idea of having a diversity of mechanisms for expressing and authenticating identity. As identity information becomes more centralized – whether through storage in a single physical location or linkage across disparate databases – there is increased likelihood for abuse.

In a networked world, the urge to link identity systems and databases together will always exist. Linking together disparate identity data may improve convenience, efficiency, and even security (in cases such as fraud detection where linking information together can help to detect and deter fraudulent activity). Linking should occur in cases where its specific benefits exceed the associated privacy and security risks. When linking is deemed necessary, strong safeguards should be erected to ensure that unnecessary linkages do not occur. These safeguards should be addressed in the design phase of an identity system (consistent with the principle of Privacy & Security By Design) and not as an afterthought.

### ✦ Proportionality

**The amount and type of identity information collected from individuals by an identity system should be proportional to the purpose for which it is collected.** This means that the amount and sensitivity of identity information required for enrollment or participation in an identity system should be reasonable and appropriate in relation to the articulated purposes of the system.

Generally speaking, it is reasonable for an identity system to collect larger amounts and/or more sensitive identity information from individuals seeking to participate in transactions of higher significance. Similarly, it is generally not reasonable for an identity system to collect a multitude of attributes, or those that divulge substantial identity information, for transactions of lower significance.

EXAMPLE 3: Gym ID Card
An athletic club might print members' names and photos on club ID cards, but collecting biometrics exceeds what may reasonably be considered necessary to ensure that only club members have access.

For many transactions, it will never be appropriate to collect certain kinds of identity information. Only in the most select of situations is it ever appropriate to ask individuals about their race, ethnicity, or religious or political affiliation, and even then this information should anonymized to the greatest extent possible.

EXAMPLE 4: College Applications
College applicants are frequently asked for race, ethnicity, or religious information for admissions purposes, but it is generally anonymized and aggregated after it is collected.

Not all transactions need to be tied to identity. Identity systems relying on pseudonymous identifiers and authentication relying on anonymous attributes should be used whenever possible.

EXAMPLE 5: IRS
The IRS may require individuals to authenticate themselves by providing their previous year's total income and a PIN number of their choice, both of which are anonymous attributes.

One way for organizations to achieve proportionality in the collection of identity information is to use trusted networks that allow individuals to leverage secure identities created through other organizations. Trusted networks reduce the number of organizations that need to collect identity information without reducing the variety of identity systems and options available to individuals.

EXAMPLE 6: OpenID
OpenID is one example of a system that provides a way for Web sites to leverage an identity created by a user through a separate "identity provider." Using this system, individuals can choose to share their identity information only with the identity provider and not with individual Web sites. When these individuals want to login to a particular blogging service, for example, the service contacts the identity provider to authenticate the individual, but the blogging service does not collect any identity information itself.

## ✦ Privacy and Security By Design

**Privacy and security considerations should be incorporated into an identity system from the very outset of the design process.** These include both safeguards for the physical system components and policies and procedures that guide the implementation of the system. Internal privacy and security practices should incorporate applicable regulatory and self-regulatory guidelines. Privacy impact assessments should be issued in conjunction with system design plans.

Identity systems should be designed with attention to human strengths and limitations that may impact the privacy and security of the systems. Knowledge of human behavior and how people will likely interact with an identity system should be incorporated from the first phases of a system's design.

EXAMPLE 7: Forgetting Passwords
People have difficulty remembering complicated passwords, so they choose passwords that are easy for others to guess. This human tendency should be central in deciding whether passwords are a strong enough authentication mechanism for the task at hand.

Consistent with the principle of Limited Use, identity systems should be designed to make secondary uses difficult. Incorporating technological and policy-based limits on the use of the system into its design will make "mission creep" – authorized but initially unintended uses – easier to avoid and less appealing later on.

Identity systems should have consistent, robust interfaces so that individuals can learn to trust legitimate systems and distinguish them from fraudulent ones.

**Principles Based on Fair Information Practices**

The remaining seven principles are adaptations of widely used fair information practices to the specific context of identity in the digital age.

### ✦ Purpose Specification

**The first step in designing an identity system should be to specify the purpose of the system and the purposes for which identity information will be collected and used.** The purposes for collecting and using identity information should be directly linked to the ultimate purpose of the system. Each purpose should have a clear and publicly communicated rationale behind it.

This specification should guide all further decisions about how identity systems will be designed, implemented, and used. Adhering to the principles of Proportionality, Limited Use, and Notice will require making decisions in accordance with the purpose specification.

### ✦ Limited Use

**Identity, authentication, and linked information should be used and retained only for the specific purposes for which they were collected.** Uses should be limited to those consistent with the identity system's purpose specification.

Secondary use, sharing, and sale of identifiers or credentials can compromise privacy and security. In particular, identification numbers can become open to privacy misuses and security threats if they are used for secondary purposes, especially in the case of authentication. Therefore, multiple uses of such identifiers should be avoided, particularly in the authentication context.

EXAMPLE 8: Social Security Numbers
The Social Security Number system was initially intended to be used for tracking income and issuing federal benefits. In the decades since it was introduced, however, the Social Security Number has been used across a whole range of other contexts, and it is now commonly used as an authenticator in setting up bank accounts, opening lines of credit, and obtaining loans. Because it is in such wide use as an authenticator, the Social Security Number has become a prime target for identity thieves and other criminals.

Use of identity, authentication, and linked information should be disclosed and minimized, and the information should only be stored until the purposes for which it was collected have been fulfilled. Identity, authentication and linked information should be shared with third parties – including data transfers between government and commercial entities – only when necessary, and should be stored by third parties only until the purpose for which it was shared has been completed.

EXAMPLE 9: Information Collection at a Bar
Consider a bar owner who decides to scan the barcodes on the backs of patrons' driver's licenses and store the names and addresses read from the barcodes in a database. The bar owner's purpose for doing this is to maintain a list of rowdy patrons who will not be allowed back to the bar. The bar owner discloses this to patrons before scanning their licenses, and turns away patrons who refuse to have their licenses scanned. To conform with the principle of Limited Use, the bar owner should not later sell his or her database to a marketer. This would constitute a use that does not conform to the purpose for which the information was collected and was not disclosed to the individuals involved.

The amount and type of data linked to an identity should be limited, and linking should occur for specific, limited and disclosed purposes.

### ✦ Individual Control and Choice

**Whenever possible, an identity system should offer individuals reasonable, granular control and choice over the attributes and identifiers needed to enroll in the system and the credentials that can subsequently be used within the system.**

Individual controls help build trust in identity systems.

EXAMPLE 10: Choices in Air Travel
There are several examples of choice in the air travel context. At U.S. airports, individuals can choose among several different government-issued identification documents for use in authenticating their identities for check-in. When checking in for a flight online, many airlines will accept several different authenticators or combinations of authenticators that reveal different kinds of identity information (first name, last name, confirmation number, credit card number, airline member number, and others).

Individuals should have the option of using a single credential or form of authentication that always discloses the same information for all interactions, or employing a variety of authentication tools for different transactions. This principle is particularly important in a system designed for both authentication and authorization, which will likely be successful only if it balances added convenience with trust in the system.

EXAMPLE 11: Control in Online Accounts
Many online services allow a single individual to maintain multiple accounts. Consider the case of a social networking site. An individual might maintain different accounts to interact with family, friends, and colleagues. Each account might be associated with different contact details, photos, and other information. The ability to maintain multiple accounts gives individuals control over not only which information is used in each context, but also which sets of information are correlated with each other. An individual may choose to put different information in an account linked to his or her real name than in a pseudonymous account.

Individuals should be given the opportunity to consent to the terms of an identity system's notice (as described in the Notice principle) prior to enrollment, authentication, or use of identity or linked information. If an individual declines to accept the notice, no information should be collected. When possible, individuals should be able to consent to participation in an identity system but decline particular terms of the notice. Should new uses of identity or linked

information be developed after an identity is created within a system, individuals should be given the opportunity to consent to or decline such uses.

Individuals should not be required to accept the sharing of information for secondary uses as a condition of enrolling in an identity system.

### ✦ Notice

**Individuals should be provided with a clear statement about the collection and use of identity, authentication, and linked information.** Notice should be conspicuous and timely, and it should be provided in a manner appropriate to the technology being used. Notice provides a basis for accountability, in accordance with the Accountability principle.

EXAMPLE 12: Cell Phone Notices
Displaying a long, multi-paged notice on a small cell phone screen is an example of how notice could be inappropriate for the technology being used.

Individuals should be notified in situations where it may not otherwise be obvious that identities are being created for them.

Prior to enrollment, individuals should be notified of:

- The purposes for which their information is being collected (as developed based on the Purpose Specification principle);
- Who is managing the identity system and creating identities for individuals within the system;
- What information will be collected and how it will be used and secured;
- How long the identity information will be stored;
- Whether and how the identity and authentication information will be used by third parties;
- What other information will be linked to the identity and whether and how that information will be used;
- Whether individuals might need to authenticate themselves in the future and how to do so;
- How the individual will be able to access and correct information related to his or her identity within the system (consistent with the Access and Data Quality principle); and
- How the individual may decline to enroll in the system.

When identity systems make use of a technology that may be unfamiliar to participants in the system, notice should be provided about the presence of the technology and its privacy implications, in accordance with the items listed above.

EXAMPLE 13: RFID
Many individuals may be unfamiliar with radio frequency identification (RFID), a technology that uses radio waves to identify and object. Individuals should be notified about how information about them – such as their location or items they have purchased – can be linked to their identities when RFID is used in an identity system.

Should new uses of identity or linked information be developed after enrollment in an identity system, individuals should be notified in accordance with the items listed above.

Individuals should be notified when other information is gathered about them and linked to their identity.

### ✦ Security

**Organizations that handle identity, authentication, and linked information should provide reasonable technical, physical, and administrative safeguards to protect against loss or misuse of the information.** Such measures should cover credentials, back-end systems that process and store information, personnel that handle the information, and physical facilities, among others.

In so doing, organizations should establish and maintain an information security program in keeping with industry standards and applicable laws, appropriate to the amount and sensitivity of the information stored in their systems. Such a security program should include processes to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of identity information; address those risks; and provide notice as appropriate for security breaches.

> EXAMPLE 14: Industry Security Standards
> ISO/IEC 17799 is one widely recognized international standard that provides best practice recommendations for information security management.

Identity systems that handle large amounts of identity information may be more vulnerable to tampering, loss, and unauthorized access (both internal and external). Adhering to strict, logical security procedures should be a top priority for such systems.

The authentication mechanism used for internal access to an identity system should be at least as strong or stronger than the mechanism for external access by participants in the system.

> EXAMPLE 15: Internal Authentication
> System administrators for a database of identity information may be required to provide two biometric credentials for authentication while participants in the system are required to provide only one biometric credential.

### ✦ Accountability

**Organizations that handle identity, authentication, and linked information should be able to verify that they are complying with applicable privacy and security protections.** Regular audits are necessary to ensure that reasonable technical, physical, and administrative privacy and security safeguards are being used. Personnel involved in handling identity information should be trained and educated about the privacy and security risks involved in dealing with identity and about applicable laws, guidelines, and procedures.

Any organization that handles identity information should include in its contracts provisions

requiring that the entities with which identity, authentication, and linked information is shared will afford that shared data a level of protection consistent with or exceeding the organization's own standards, consistent with these principles and any industry standards that conform to these principles.

EXAMPLE 16: Industry Standards for Shared Information
The PCI Data Security Standard is an example of an industry standard that can be implemented via contracts between entities sharing identity information.

### ✦ Access

**Individuals should be provided reasonable access to the identity, authentication, and linked information that organizations maintain about them and use in the ordinary course of business.** This ability should be secured against unauthorized access.

The information should be easy for individuals to access, view, understand and change. Individuals should also be able to challenge conclusions drawn from identity and other information via structured and impartial processes. Whenever possible, individuals should be able to see when their identity information has been disclosed and to whom.

Depending on the context, access should either be provided by the organization that enrolls the individual or the organization interfacing with the individual, if they are different.

### ✦ Data Quality

**Organizations should strive to ensure that the identity information they hold is timely, complete, and accurate.**

Individuals should be able to correct inaccurate, out-of-date, and incomplete information. The data quality principle may thus be partly dependent on the access principle, since individuals will need to access their information in order to correct it.

## III. GLOSSARY

Italicized definitions are from the National Research Council's *Who Goes There? Authentication Through the Lens of Privacy*.[1]

*Attribute. An attribute describes a property associated with an individual.*

*Authentication. Authentication is the process of establishing confidence in the truth of some claim.*

Authentication Information. One or more facts presented to support the authentication of an identity.

*Authorization. Authorization is the process of deciding what an individual ought to be allowed to do.*

*Credential. Credentials are objects that are verified when presented to the verifier in an authentication transaction. Credentials may be bound in some way to the individual to whom they were issued, or they may be bearer credentials. The former are necessary for identification, while the latter may be acceptable for some forms of authorization.*

Enrollment. Enrollment is the process by which an identity for individual X is created in identity system Y.

*Identification. Identification is the process of using claimed or observed attributes of an individual to infer who the individual is.*

*Identifier. An identifier points to an individual. An identifier could be a name, a serial number, or some other pointer to the individual being identified.*

*Identity. The identity of X is the set of information about individual X, which is associated with that individual in a particular identity system Y. However, Y is not always named explicitly.*

*Identity Authentication. Identity authentication is the process of establishing an understood level of confidence that an identifier refers to an identity. It may or may not be possible to link the authenticated identity to an individual.*

Identity Information: One or more attributes used to establish an identity.

Identity System: Any program or framework that involves the collection, authentication, or use of identity or linked information. Identity systems may be designed, implemented and used by government, businesses, or individuals.

*Individual Authentication. Individual authentication is the process of establishing an understood level of confidence that an identifier refers to a specific individual.*

Linked Information: Other facts about an individual, such as transactional, shopping or travel behavior, tied to an identity.

---

[1] National Research Council of the National Academies. *Who Goes There? Authentication Through the Lens of Privacy*. Eds. Stephen T. Kent and Lynette I. Millett. Washington: The National Academies Press, 2003.

Pseudonymous: Using a name or label that may identify an individual within a system but does not correlate to that individual outside of the system.

Secondary Use (of information): Any use of identity or linked information that is inconsistent with an identity system's purpose specification.

Use (of information): Any use of identity, authentication, or linked information other than for enrollment and authentication purposes. Use may follow either enrollment or authentication.

**Before the**

**FEDERAL COMMUNICATIONS COMMISSION**

**Washington, D.C. 20554**

| | | |
|---|---|---|
| In the Matter of | ) | |
| | ) | |
| A National Broadband Plan for our Future | ) | GN Docket Nos. 09-47, 09-51, 09-137 |
| Comments – NBP Public Notice #29 | ) | |
| | ) | |
| | ) | |

**COMMENTS OF THE CENTER FOR DEMOCRACY & TECHNOLOGY: APPENDIX E**

**Issues for Responsible User-Centric Identity, A White Paper by the Center for Democracy & Technology, November 2009**

One of the central challenges of the digital age is creating, managing, and sharing digital identities online. As online interactions become richer and more complex, individuals are asked to identify themselves increasingly often - using their name, their address, or simply an identification number to correlate their visits. In addition, services online are increasingly being offered subject to user authentication; for example, users can use a credit card to make a purchase or file their taxes online, as long as they can prove their identity. As the use of authentication increases, so does innovation around online identity. However, these innovations must be considered thoughtfully in order to ensure that they are protective of the user, building trusted online relationships.

The U.S. government is launching a series of pilot programs that will use third party user credentials to authenticate users to federal Web sites in order to provide a better user experience. Using third parties to authenticate users makes sense in many ways, allowing users to use credentials they already have (rather than yet another set of user name and password) and allowing agencies to free up development resources for other tools, instead of maintaining their own sign-on system. In order to work with the government, these third party identity providers must adhere to a trust framework that sets a minimum level of best practices for the identity provider. However, creation of robust trust frameworks for government use, as well as for general use, requires that identity providers and trust framework providers work together to answer a set of questions around the provision of identity and services online.

## I. Background

In the digital context, identity is simply a claim or set of claims about the user, similar to the physical claim of a driver's license ("this person is allowed to drive according to this state") or a library card ("this person is allowed to borrow books"). This identification is often subject to authentication - that is, the process to verify that the identification is, in

fact, true. The process of claiming identity, authenticating identity, and authorizing that identity to use certain services is known as Identity Management.

Traditionally, identity exchange has been a direct interaction between a user and the service provider. This model is evolving as Web services and Internet applications now frequently require new forms of identity information. Some of these new models for identity management place the user in the middle of an interaction between an identity provider and an online service. This method, called Federated Identity, allows service providers to rely on trusted third parties to authenticate users of their service. Often, this eases use for users by reducing the number of sign-in credentials they must remember.

Many of the federated identity technologies developed to address problems with traditional identity solutions fall under the loosely defined term "user-centric identity." This term refers to systems where users, rather than service providers, control their identity credentials. This is a closer metaphor to the offline world, where we carry a variety of identity documents issued by different authorities, and choose which identity credential or authenticator to present in each transaction. These new online systems must be designed with privacy and security as foremost concerns due to the often-sensitive nature of the information held by the identity provider.

User-centric federated identity systems have the potential to improve the security and privacy of authentication and services for users; however, if improperly designed, these systems can negatively impact users and prove a burden instead. CDT believes that user-centric federated identity has great promise to make online interactions easier, more secure, and more easily controlled by the user. There is skepticism from privacy and security advocates that user-centric federated identity will be implemented in ways that maximize the potential of these technologies for consumers, industry, and government. We hope to serve as advisors on policy matters in order to ensure that the promise of user centric federated identity is maximized as we move towards implementation of these federal government pilot programs.

## II. User-Centric Identity

Whereas in traditional systems users directly exchange identity information with service providers, the relationships within a user-centric federated identity system is becomes more complicated:

1. The *trust framework provider* creates a trust framework with a set of minimum practices that must be upheld in order to be considered trusted within the framework, and evaluates identity provider practices against this framework.
2. The *identity provider* manages the user's identity information and provides authentication of the user to service providers.
3. The service provider, also referred to as the *relying party*, provides a service to the user, based on identity information provided by an identity provider.
4. The *user* registers his or her identity information with one or more identity providers and controls how that information is shared with service providers.

Central to the vision of these technologies is that there is no single central identity provider. There can be a variety of competing identity providers offering services tailored

to particular needs of both users and relying parties. Robust competition in this market will potentially give users greater choice and control over how they manage their personal information in online transactions. In some cases users themselves may act as the identity provider.

*Figure 1: Traditional Identity Authentication*

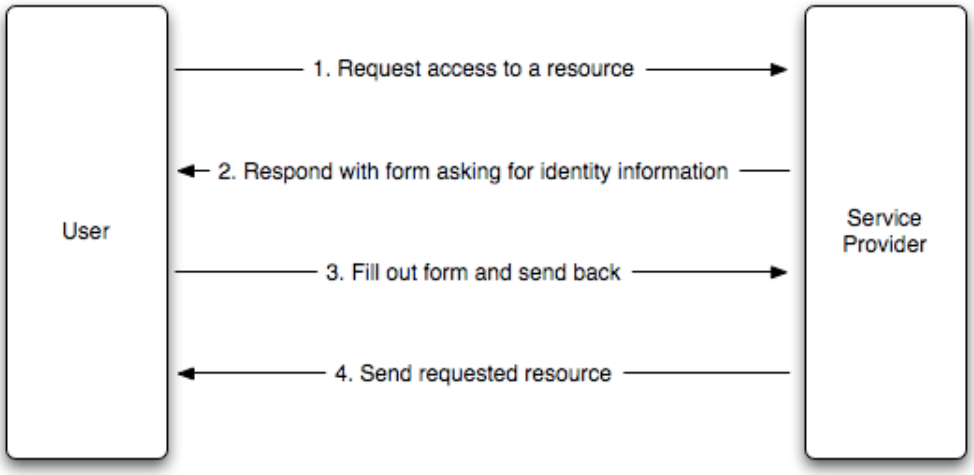
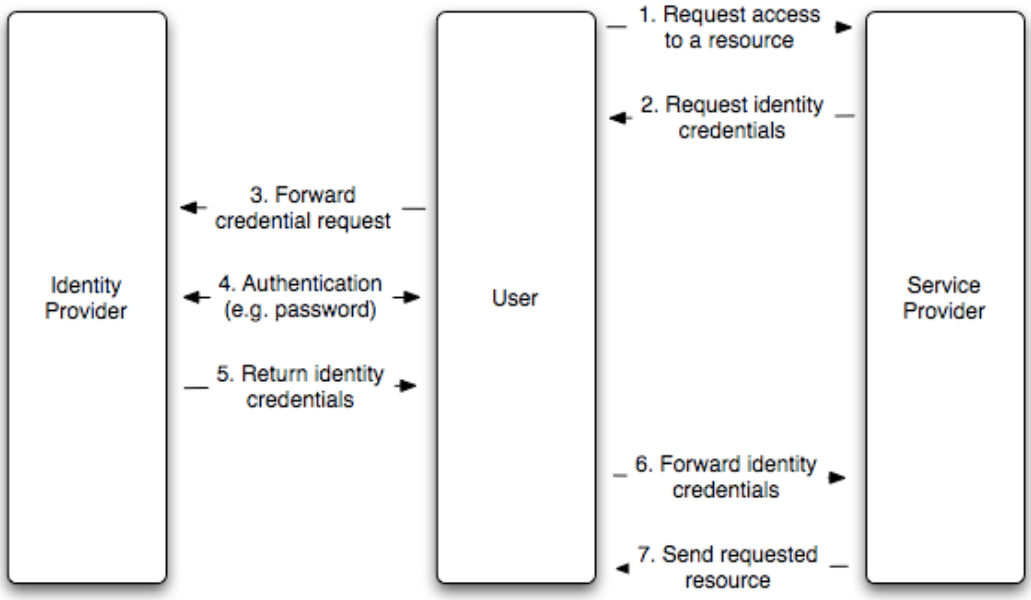



*Figure 2: User-Centric Identity Authentication*




In a user-centric federated identity transaction, a credential is passed between the identity provider, the user, and the service provider. This credential is a secure message stating "Identity Provider X certifies that the holder of the credential satisfies Y," where Y might be "user name is 'JohnDoe'," or even "the user works for Widgets Inc." This credential is useful to the service provider only to the extent that it trusts the identity provider. Low-sensitivity services might trust any identity provider that correctly follows

the protocol outlined in a trust framework or identity schema. High-sensitivity uses might require well-known identity providers that do offline verification of the data they provide.

## III. Benefits and Liabilities in Federated Identity Management

Using a third-party identity provider has benefits for both the user and the service provider. The service provider is freed from the significant effort required to manage user accounts, verify identity claims, and reset forgotten passwords. Users benefit from not having to register with each new service provider, and not having to remember separate user names and passwords.

However, introducing a third party that uses personal information to interact with so many online services on behalf of the user introduces new privacy and security concerns. In order to benefit from user-centric identity systems, users must disclose personal information to identity providers and relying parties. The benefits of user-centric identity to both users and relying parties will be lost if users do not have sufficient confidence that their information will be protected against unauthorized use or disclosure (and confidence in avenues for redress to deal with subsequent harms that may flow). These risks apply not only to information provided by users to identity providers and relying parties, but also information collected from third parties about the user and transaction data about users generated as a result of their online activities. Without strong privacy and security protections, users are exposed to a host of harms---for example, identity theft, unauthorized account access, and embarrassment.

Third party management of personal information also raises key questions around how to best allocate legal obligations and liability among the parties to both encourage robust competition in this market and protect the privacy and security of user data. One category of potential liability centers on the misuse or unauthorized disclosure of user information. By using a third party to manage user information, relying parties may be freed from some legal requirements and liability. However, the identity provider may assume more liability and risk. Potential liability may arise where there is a faulty identification, faulty authentication, or failure to follow trust framework procedures. Users and relying parties can suffer harm and potential liability where a relying party acts on a faulty identity credential it thought was valid, or fails to act on a credential it believes is faulty. Users can also suffer harm when they are denied access or authorization to a service they are actually entitled to because of improper action by either the identity provider or relying party.

In addition, the relying party may still aggregate information about a user, in which case liability and legal requirements are not removed. In fact, additional burdens may be placed on the relying party as part of a trust framework or as part of a transaction with the trust provider, in order to ensure that the relying party does not require unnecessary information to be passed.

## IV. U.S. Government Pilots

The newest entrant into the user-centric identity field is the U.S. Government, having recently announced three pilot programs using user-centric federated identity

management to improve access to government information while leveraging existing credentials for users. These pilots will be held through the Center for Information Technology (CIT), the National Institutes of Health (NIH), and the U.S. Department of Health and Human Services (HHS).

The Identity, Credential and Access Management group (ICAM) has developed a set of schemas for the adoption of trust frameworks for use in government[1]. These trust frameworks will govern the operations of, policies of, and relationships between identity providers, users, and federal Web sites. Once ICAM and the GSA approve a trust framework, the trust framework may certify identity providers as compliant with their trust framework, and in turn federal sites involved with the pilot will be able to accept credentials from these identity providers.

Trust frameworks establish the conditions under which individual identity providers (and perhaps their relying parties) will qualify for participation in a federated system for collection, exchange, and authentication of user information. In addition, the trust framework determines how trustworthy a given credential is, determining what kinds of services it can authorize on federal Web sites. In order to be trusted by the government pilot, an identity provider must be operating as part of a trust framework approved by the ICAM Trust Framework Adoption Process. Currently, OpenID Foundation, Information Card Foundation, Kantara Initiative, and the InCommon Federation are active in this process. The trust framework provider must ensure that each identity provider that they certify is behaving within the bounds of the trust framework.

These trust frameworks are adopted based on the level of certainty that they can provide. The adoption process compares the trust framework to the applicable federal requirements, policies, and laws. As part of this adoption process, a Scheme Profile that determines how the federal government will use the identity profile created by each trust framework, how secure it is, and what level of authentication it can provide. Each Scheme Profile is then matched against the levels of assurance defined in OMB Memorandum 04-04[2], which sets out levels of assurance that are necessary for government transactions:

- Level 1: Little or no confidence in the asserted identity's validity (for example, used to personalize federal Web sites for users or allow participation in government discussions online; pseudonymous)
- Level 2: Some confidence in the asserted identity's validity (for example, changing an address of record)
- Level 3: High confidence in the asserted identity's validity (for example, submission of proprietary patent information, or disaster management information for first responders)
- Level 4: Very high confidence in the asserted identity's validity (for example, law enforcement criminal records databases or health records from the VA)

---

[1] Materials released by ICAM can be found at idmanagement.gov, including relevant memorandum.

[2] M-04-04 "E-Authentication Guidance for Federal Agencies" < http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf>

Each of these levels is determined based on the information needed by the particular Web site or application, the importance and sensitivity of the services, and the potential harms.

While these government pilots are driving trust framework creation in user-centric identity, it is expected that User Centric Identity Systems will be used extensively for purposes unrelated to government sites. Accordingly, the development of these trust frameworks raises questions that go far beyond what minimum requirements the government might impose as a condition to treating a particular identity provider or trust framework provider as acceptable for access to government sites at any particular level of assurance.

## V. Key Initial Policy Questions for User-Centric Trust Framework Providers

The direction that is taken on key policy questions in these trust frameworks for federal use may well shape the direction for the operations of user-centric identity for the near future. Key in the development of a trust framework is the creation of a set of minimum conditions that must be met by each participating identity provider, and how the trust framework will certify (and decertify) each provider. In addition, the responsibilities, obligations and liabilities of the trust framework provider, the identity provider, the relying party, and the user must be made clear. Establishing an appropriate set of rules around these minimum obligations can create trust for users, increase user adoption of these services, and make it significantly easier to establish relationships online.

There are several options for shaping an appropriate set of rules between the framework, the identity provider, the relying party, and the user. Traditionally, terms of service and privacy policies created and posted by Web sites define various rights and responsibilities of the Web site in regards to user data. Often, user responsibilities are also included. However, these terms and policies are rarely understood and do not address the obligations of or relationships to third parties.

Current privacy policies and terms of service are simply not effective for this kind of practice. Identity management across many Web sites carries new privacy risks and more data and information than other kinds of services, and users must be given greater control over their information.

Legislation or regulation might be used to establish mandatory practices among the members of a federated identity management. However, this approach would not deal well with the evolution of services online. Legislation and regulation should likely be the last resort if key players do not move promptly and responsibly to address privacy protections and key aspects of user-centric governance.

The provision of identity services via trust frameworks raises many policy questions. A promising way to resolve these issues would be for the Trust Framework to impose, as a condition of participation, some minimum terms that would govern the interactions among all three parties – the Identity Provider, the Relying Party and the User. Such mandatory contract terms might be made enforceable by each of the parties against the other, thereby reducing burdens on the trust framework provider.

One way or another, these will be addressed in the context of implementation decisions. These decisions will determine the level of risk to privacy and security for users and the types of liability and redress for potential harm that may exist for each member of the federated identity system.

Trust framework providers

1. *Admitting identity providers*: On what basis will the trust framework will certify identity providers as meeting a minimum standard? Will the assertions made by the identity provider be trusted, or will an audit of identity provider practices be performed? On what basis could a trust framework decline to admit a new member?
2. *Auditing identity providers*: If identity providers must be audited, who will do the audit, what independence criteria might apply, and to whom will the auditor owe an obligation?
3. *Showing compliance*: Will the framework give identity providers a way to show compliance with the framework, such as a mark or seal? With what resources and how will compliance be policed?
4. *Setting framework policy*: How will the trust framework policy be set, and by whom? How will user interested be taken into account, and how will policies be communicated to users? How will policies evolve?
5. *Breach of service*: If an identity provider were to breach its obligations within a trust framework, what would be the consequences?

Minimum rules for identity providers

1. *Trust framework requirements*: Will the trust framework require some minimum contract with the identity provider in order to constrain the terms that the identity provider can provide the user?
2. *Relationship to trust framework*: What will the relationship between the identity provider and the trust framework provider be? Will it be contractual, and will it also involve the user and relying party?
3. *Relationship to relying party*: Will identity providers exercise any discretion regarding with which Relying Parties they will deal? Will the provision of authenticated information to Relying Parties carry with it any obligation or potential liability for relying parties or identity providers (other than an obligation to provide information believed in good faith to be accurate)?
4. *Relationship to user*: Will identity providers be subject to some minimum requirements regarding the privacy and security of information regarding users? Will there be data retention or use limitation policies?
5. *Obligations with information passage*: Will relying parties be subject to some obligations as a condition of getting access to information about the user?

Recourse and Liability

1. *Liability of and obligations to the user*: If an identity provider fails to provide the expected services or fails to meet their obligations under the trust framework, and users are harmed, will there be any user recourse? If user information is misused or disclosed without authorization, what rights does the user have? Does the user bear liability for providing false identity information?
2. *Liability of the identity provider*: What is the liability of the identity provider of a faulty identification or faulty authentication? For failing to adequately protect user information against unauthorized use or disclosure?

3. *Liability of the relying party*: What is the liability of the relying party for relying on a faulty authentication (for example, in the case of identity theft) or rejects a valid credential it mistakenly believes is compromised? For failing to adequately protect user information against unauthorized use or disclosure?
4. *Obligations to trust framework*: If the trust framework imposes minimum contractual obligations, who will be entitled to enforce the contract? Will there be any obligation to enforce the contract?
5. *Dispute resolution procedures*: What dispute resolution procedures would be available for disputes between identity providers and trust framework provider? Between identity provider and trust framework? For the user, with respect to any of the parties?
6. *Accuracy*: Is there a method in place to allow the accuracy of information to be determined? Is there a way for a user to correct the record?

Privacy and Security

1. *Data minimization*: Is there a limit on the scope of information that may be collected (by any party) about the user? Is there a limit on the length of time that data is retained, and how is it destroyed?
2. *Purpose specification and use limitation*: Are there limitations on how information collected can be used by any party?
3. *Transaction authorization*: Will identity services provide the User with the option to approve or decline submission of authenticated information to a relying party in every instance? Can uses prohibit particular users of certain information?
4. *Security*: Will identity providers or relying parties be subject to minimum requirements on the security of data? What governance mechanisms will be imposed to prevent against unauthorized use or disclosure?
5. *Courts*: What standards apply to law enforcement access or disclosure associated with civil litigation?

Each set of questions must be resolved while establishing the obligations within a user-centric identity regime. Any such regime must impose and enforce a set of rules that increase trust for identity providers within the regime.

## VI. Conclusion

If trust framework providers can establish an appropriate set of rules regarding the minimum obligations of identity providers, relying parties and users, there is a large potential to increase the ease with which trust relationships can be formed online. Particularly for single transactions between parties who do not otherwise know each other, UCI systems have the potential to reduce transaction cost and risk. And, indeed, they may even be useful in enabling the formation of more online communities.

However, this model can only be successful if privacy and security are adequately protected and risks and liability are allocated in such a way as to enable enforcement and encourage user adoption.

The development of trust frameworks for user centric identity provides a unique opportunity to design truly user-centric and privacy protective identity management

regimes. These design decisions will determine the ease of use, liabilities, and obligations between each player in the federated identity.

Determining the obligations of each party interacting within the auspices of a trust framework will be the key aspect of creating a trust framework. Creating strong relationships between each of the parties in a user-centric federated identity system will in turn create stronger, more trusted relationships online.

Any set of answers to questions about identity must:

- impose and enforce some set of rules that increase trust in associated identification services, thereby enabling productive transactions between strangers.
- allow flexible evolution of the relevant services and support an adequate business model for participants.
- be robust against fraud or manipulation, protect the privacy and security of User data, and provide appropriate avenues for dispute resolution, redress, and/or liability in the event of performance failure.
- be adequately open to new participants without eliminating minimum qualifications and rules.