KEEPING THE INTERNET
OPEN • INNOVATIVE • FREE

www.cdt.org

CENTER FOR DEMOCRACY
& TECHNOLOGY

1634 I Street, NW
Suite 1100
Washington, DC 20006

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

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

---

[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.

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 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.*

---

[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.

[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").

- **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.*

- **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.

[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").

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 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

---

[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.

[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.

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 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.

---

[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.

[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").

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 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]

---

[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").

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 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

---

[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.

[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.

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 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

---

[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.

[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.").

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]

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

---

[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.

[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.

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 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

---

[33] DHS FIPs.

[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.

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.

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

[35] NAI Principles.

[36] IAB Principles.

[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.

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 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]

---

[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.").

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 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.*

[42] *Id.*

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.

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

[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.

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 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.

---

[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).

[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.

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.*

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

[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").

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.

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

---

[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.").

[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).

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.