Testimony of
Berin Szoka, President
TechFreedom[1]

on

"The Need for Privacy Protections: Is Industry Self-Regulation Adequate?"

Before the Senate Commerce Committee[2]
June 28, 2012

I. Introduction

Chairman Rockefeller, Ranking Member Hutchison—thank you for inviting me to testify about privacy again before your Committee. As President of TechFreedom, a non-profit think tank, and before that, as Director of the Center for Internet Freedom at The Progress & Freedom Foundation, I have worked for over four years to articulate an alternative perspective on privacy that recognizes both the enormous value created by data and the need to prevent abuses of data. The debate thus far has systematically underestimated the benefits to consumers from the use of personal data to tailor advertising, develop new products, and conduct research, while overstating the dangers of data, which remain largely conjectural.

With the best of intentions, we are heading towards reshaping the fundamentals of the Internet—in ways that may have serious negative unintended consequences for privacy, the sites and services consumers enjoy, and the health of the ecosystem. But the *way* we're doing it may be even more troubling. This is not the result of a bottom-up evolutionary process, but of collusion between government and powerful market players. We are heading for opt-in dystopias.

II. The American Layered Approach to Privacy

I agree that self-regulation is not enough, that so-called "baseline" legislation is, indeed, necessary. I disagree, however, that *new* baseline legislation is needed. We already have baseline consumer protection legislation: Section V of the Federal Trade Commission Act[3] empowers the FTC not only to enforce self-regulation by holding companies to their promises,

---

1 Berin Szoka (@BerinSzoka) is President of TechFreedom, a non-profit, non-partisan technology policy think tank. He has written and commented extensively on consumer privacy. In particular, he testified on Balancing Privacy and Innovation before the House Energy & Commerce Committee, Subcommittee on Commerce, Manufacturing, and Trade on March 29, 2012, available at http://tch.fm/KCrz8k, ("Szoka Testimony").

2 http://commerce.senate.gov/public/index.cfm?p=Hearings&ContentRecord_id=aa018084-ceea-472c-af63-97d7f44fac80.

3 15 U.S.C. § 45 (2006).

but also to prohibit as "unfair" uses of personal data that do more harm than good and that consumers themselves cannot reasonably avoid. States have similar legislation, empowering Attorneys General to act,[4] and class action lawsuits also deter privacy violations.[5]

On top of this baseline, we have built a layered approach to privacy protection. Where the FTC's authority has proven inadequate, Congress has enacted legislation to address specific problems, such as the Children's Online Privacy Protection Act[6] and the Fair Credit Reporting Act.[7] But in general, American law follows a common law model, addressing problems on a case by case basis rather than attempting to design a comprehensive regulatory scheme adequate for both present and future. This is what Richard Epstein famously called "Simple Rules for a Complex World."[8] The Electronic Frontier Foundation's Mike Godwin put it best in 1998 when he said: "It's easier to learn from history than it is to learn from the future. Almost always, the time-tested laws and legal principles we already have in place are more than adequate to address the new medium."[9]

Applying baseline principles of consumer protection is the best way to address new privacy challenges, given the ever-changing nature of the technologies involved and the inevitable trade-offs among competing conceptions of privacy, and between privacy and other values—such as:

- Funding for innovative media and services that would not otherwise be available;
- The diversity and competitiveness of an Internet ecosystem with low barriers to entry;
- The ease of use for consumers of an Internet that is not divided by checkpoints asking for consent or payment as users cross domain name boundaries;
- The innovation driven by discoveries made possible by analyzing what some have pejoratively labeled "Big Data," and so on.

Policymakers simply do not have the expertise or foresight to make complex rules to decide these trade-offs—or the time to become experts in complex technologies. So it is here that self-regulation plays a critical role in our layered approach to privacy. As the White House

---

4 Henry N. Butler & Joshua D. Wright, Are State Consumer Protection Acts Really Little-FTC Acts?, 63 Fla. L. Rev. 163, 165 (2011) (discussing state laws empowering attorneys general to "combat consumer fraud and other deceptive practices").

5 Glenn G. Lammi, "Thanks, Google Buzz: Class Action Lawyers Celebrate Impending Fees," Forbes,Nov. 3, 2010, available at http://www.forbes.com/sites/docket/2010/11/03/thanks-google-buzz-class-action-lawyers-celebrate-impending-fees/.

6 Children's Online Privacy Protection Act of 1998, Pub.L. No. 105-277, 112 Stat. 2581-728 (codified in 15 U.S.C. §§ 6501–6506).

7 Fair Credit Reporting Act of 1970, Pub. L. 91-508; 84 Stat. 1128 (codified in 15 U.S.C. § 1681).

8 Richard A. Epstein, Simple Rules for a Complex World (1995).

9 Quoted in Virginia Postrel, The Future and Its Enemies: The Growing Conflict Over Creativity, Enterprise, and Progress at 48 (Touchstone 1998).

privacy report acknowledged, self-regulation alone "can provide the flexibility, speed, and decentralization necessary to address Internet policy challenges."[10]

In short, self-regulation is necessary, but not sufficient. It must work in tandem with the enforcement of existing laws—which I believe can be enhanced significantly *without* new legislation. But we must also understand that self-regulation is merely one part of a broader process by which market forces discipline corporations in how they collect, process, use and distribute personal data about us. Together, this layered approach is the best way to maximize the enormous benefits offered by the use of personal data while minimizing its occasional abuse.

III. Market Regulation of Privacy

Companies do not operate in a vacuum. They compete not just for customers, but to protect their good name in the eyes of business partners, shareholders, media watchdogs, potential employees, and citizens themselves. Nowhere in the economy is this more true than online, where companies compete both for consumers' attention and for the trust of business partners, especially advertisers.

The social media revolution has made it possible for anyone concerned about online privacy to blow the whistle on true privacy violations. That whistle may not always be loud enough to be heard, but it's more likely in this sector than any other. Traditional media sources like the Wall Street Journal have played a critical role in attracting attention to corporate privacy policies through "What They Know" series,[11] which has been popularized using social media tools. Reporters like Julia Angwin may rightly lament the failure of self-regulation in any particular case, but the very act of their criticism is essential for *market* regulation to function, because they are powerful actors in the marketplaces of ideas and reputation.

Earlier this year, social media tools were directed at Congress—to great effect—to express grassroots concern about the impact of proposed copyright legislation. While some Internet companies certainly helped to promote these messages, even were it not for their involvement, this experience would demonstrate how effective social media activism can be. There is no reason why such techniques cannot be used effectively against major Internet companies themselves, just as Facebook users have used Facebook itself to rally opposition to Facebook on privacy concerns such as its Beacon ad targeting system.[12] "The herd will be heard," as Bob

---

[10] The White House, Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy at 23, http://www.whitehouse.gov/sites/default/files/privacy-final.pdf.

[11] *See generally What They Know*, Wall St. J., 2012, http://blogs.wsj.com/wtk/.

[12] See, e.g., Kirsten E. Marti, Facebook (A): Beacon and Privacy 3 (2010), available at http://www.darden.virginia.edu/corporate-ethics/pdf/Facebook%20_A_business_ethics-case_bri-1006a.pdf ("The online community responded immediately to this intrusion. MoveOn.org created a Facebook group "Petition: Facebook, stop invading my privacy!" that stated: "Sites like Facebook must respect my privacy. They should not tell my friends what I buy on other sites—or let companies use my name to endorse their

Garfield memorably put it in his 2009 book, *The Chaos Scenario: Amid the Ruins of Mass Media*.[13] The Choice for Business Is Stark: Listen or Perish. Among the most important factors driving companies to participate constructively in the multi-stakeholder process, to forge meaningful privacy protections, and to abide by them is the fear of a Wall Street Journal article, a social media frenzy, or organized campaign demanding action on a particular privacy problem.

As Wayne Crews of Competitive Enterprise Institute put it in testimony before this committee in 2008:

> Businesses are disciplined by responses of their competitors. Political regulation is premature; but "self-regulation" like that described in the FTC principles is a misnomer; it is competitive discipline that market processes impose on vendors. Nobody in a free market is so fortunate as to be able to "self regulate." Apart from the consumer rejection just noted, firms are regulated by the competitive threats posed by rivals, by Wall Street and intolerant investors, indeed by computer science itself.[14]

IV. Enhancing the American Layered Approach to Privacy

As I argued in March in testimony before the House Energy & Commerce Committee's Subcommittee on Commerce & Manufacturing,[15] the FTC could do much more with its existing authority to build an effective quasi-common law of privacy in three ways.

First, Congress should assess whether the FTC has adequate institutional resources and expertise. If the FTC had heeded my fellow panelist Peter Swire's call for the FTC to build a an office of information technology five years ago,[16] our layered privacy approach would today be far more effective in protecting consumers and ensuring their trust, and less easily dismissed as inadequate by foreign privacy regulators. Chairman Leibowitz deserves credit for appointing the agency's first Chief Technologist. But even with someone as talented as Ed Felten in that position, the FTC is still way behind the curve: His title is not Chief Technology *Officer* because there is no office behind him.

---

products—without my explicit permission." The Facebook group and petition had 2,000 members within the first 24 hours and eventually grew to over 80,000 names." [internal citations omitted]).

[13] James Cherkoff, "The Joy of a Gated Community," The Chaos Scenario, June 1, 2010, http://thechaosscenario.net/.

[14] Wayne Crews, Testimony Before the Senate Committee on Commerce, July 9, 2008, *available a*t http://cei.org/sites/default/files/Wayne%20Crews%20-%20Senate%20Commerce%20Testimony%20-%20Online%20Advertising,%20July%209%202008.pdf.

[15] Berin Szoka, Testimony Before the House Energy & Commerce Committee, Subcommittee on Commerce, Manufacturing, and Trade, "Balancing Privacy and Innovation: Does the President's Proposal Tip the Scale?", Mar. 29, 2012, available at http://techfreedom.org/sites/default/files/Szoka%20Privacy%20Testimony%20to%20CMT%203.29.12%20v3%20(final)_0.pdf.

[16] Peter Swire, *Funding the FTC: Globalization and New Information Technologies Necessitate an Appropriations Boost*, Feb. 26, 2007, http://www.americanprogress.org/issues/2007/02/ftc.html.

The FTC needs a clear strategic plan outlining (a) how to build the in-house technical expertise it needs (beyond basic IT infrastructure) to identify enforcement actions, support successful litigation, monitor compliance, and conduct long-term planning and policy work, and (b) the resources necessary to achieve that goal through a combination of re-prioritizing current agency spending and additional appropriations. Importantly, this organization should function as a cohesive team that meets the needs for technical expertise of all the FTC's bureaus and offices (including the Bureau of Competition). A stand-alone organization could, like the Bureau of Economics, better attract and retain talent.

Second, the clearer privacy promises are, the more easily the FTC will be able to enforce them. One important way to achieve this goal would be for the FTC to promote the use of "smart disclosure"—the term used by Cass Sunstein, director of the Office of Information and Regulatory Affairs and a close advisor to President Obama, and a widely respected thinker in law, policy and technology. Smart disclosure can empower consumers by letting software do the work for them of reading privacy policies—and then implement their privacy preferences.

For example, users could subscribe to the privacy recommendations of, say, Consumer Reports, or any privacy advocacy group, which in turn could set their phone to warn them if they install an app that does not meet the privacy practices those trusted third parties deem adequate. Or, more simply, such a system could work for communicating whether a site, service or app acedes to a particular self-regulatory code of conduct—and phone privacy controls could be set by default to provide special notices when users attempt to install apps that do not certify compliance with self-regulatory codes of conduct. As the FTC Privacy Report notes, smart disclosure could also "give consumers the ability to compare privacy practices among different companies."[17] An app store might illustrate how such comparisons could work, allowing users trying to choose between several competing apps to compare their privacy practices side by side.

While it would be preferable for smart disclosure to arise through self-regulation, especially given the complexity of crafting disclosure formats, mandating disclosure of privacy practices would generally be a better way for government to address demonstrated market failures than by dictating what constitutes fair information practices—and thus might be an appropriate area for Congress to explore legislation at some point.

Third, the proper measure of the FTC's effectiveness is not how many suits it successfully settles, but how well it contributes to the development of a quasi-common law of privacy that can guide companies pushing the envelope with new data-driven technologies—without stifling innovation that ultimately serves consumers. The chief problem today is that companies have only FTC complaints and consent decrees to guide in predicting the course of the law. These documents offer very little explanation of how the facts of a particular case satisfy the FTC's Policy Statements on unfairness and deception. And these summary assertions are never

[17] Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers* 62 ("FTC Report"), http://www.ftc.gov/os/2012/03/120326privacyreport.pdf.

tested in court, both because of the cost of litigation relative to settlement, and because of the cost to a defendant company of bad publicity from being perceived as anti-privacy exceed the benefits of taking the FTC to court—even when they would likely prevail given the FTC's overreach. While this should reassure us that reputation markets exert far greater pressure to discipline companies on privacy than is commonly appreciated, it also means that we lack the key ingredient for building a true common law: judicial scrutiny in an adversarial process.

The forces that keep privacy adjudication out of the courts and prevent development of privacy common law by judges are not likely to be easily overcome by FTC—or even Congressional—action. So we need to find alternative ways to replicate the adversarial process of careful analysis by which courts build upon simple rules to address the challenges of a complex world. I suggest the following six possible ways for the FTC to make better use of its existing authority to build a quasi common law:

1. The Commission (or individual Commissioners) should provide greater analysis of its rationale under its Unfairness and Deception Policy Statements for issuing each consent decree.
2. The FTC should, when it closes an investigation by deciding *not* to bring a complaint, issue a "no action" letter explaining why it decided the practice at issue was lawful under Section V.[18] Such letters, issued by other agencies like the Securities and Exchange Commission, provide an invaluable source of guidance to innovators. Congress should even consider whether the FTC should be required to issue such letters.
3. The FTC should consider how it could use advisory opinions more effectively to provide guidance to industry on how the agency might evaluate new privacy practices—especially for companies working on the cutting edge of technology, which are often small. The FTC issues such letters on a wide range of topics,[19] yet does not appear to have issued advisory opinions regarding the application of Section V to privacy.
4. Congress should reassert the vital oversight it exercised in 1980 and 1983 when it ordered the agency to issue the Policy Statements on Unfairness and Deception. At a minimum, the FTC should be required to explain, in detailed analysis, how it has applied those venerable standards in past privacy enforcement cases, and how it plans to do so in the future—again, because it is "easier to learn from history than it is to learn from the future."[20] Such guidelines are routine in other areas, and provided for in the

---

[18] *See, e.g.,* Jodie Bernstein, *Re: Petition Requesting Investigation of, and Enforcement Action Against SpectraCom, Inc.*, http://www.ftc.gov/os/1997/07/cenmed.htm.

[19] 16 C.F.R .§ 1.1 (2012) ("Any person, partnership, or corporation may request advice from the Commission with respect to a course of action which the requesting party proposes to pursue. The Commission will consider such requests for advice and inform the requesting party of the Commission's views, where practicable, under the following circumstances... (1) The matter involves a substantial or novel question of fact or law and there is no clear Commission or court precedent; or (2) The subject matter of the request and consequent publication of Commission advice is of significant public interest."); *see also* Judith A. Moreland, *Overview of the Advisory Opinion Process at the Federal Trade Commission*, *available at* http://www.ftc.gov/bc/speech2.shtm.

[20] *See supra* note 9.

Commission's current procedures.[21] Indeed, the antitrust guidelines issued by the FTC and DOJ form a key element of the American common law of competition. The FTC has issued a number of Guides[22] to explain its approach to consumer protection—but none for consumer privacy.[23] The FTC's recently issued privacy report is no substitute for such a Guide—indeed, it has little grounding in the twin Policy Statements that are supposed to be the FTC's lodestars. To replicate some of the adversarial nature of actual litigation, the process must be the result of a substantive dialogue with affected stakeholders, and it must be subject to involved oversight from the full Commission and from Congress.

5. In particular, the FTC must clarify the boundaries of privacy harm under the Unfairness Doctrine. The FTC's leadership seems to to be trying to have it both ways: playing down publicly what they can do with their existing legal authority (to support their argument for new statutory authority) while, at the same time, making bold claims about the scope of harm in their enforcement actions. If the concept of harm is stretched too far, the Unfairness Doctrine will become again, as it was in the 1970s, a blank check for the FTC to become a second national legislature.[24] I explain my concerns about the potential for the unfairness doctrine to be abused, but also my belief that the doctrine should be used to the greatest extent degree with the 1980 Policy Statement, in my March testimony before the House Energy & Commerce Committee.[25]
6. Congress should ensure the FTC has the resources adequate to engage in this detailed analysis. To dismiss the current legal model as inadequate simply because it has not been fully utilized, and to adopt instead a new legislative framework whose true costs are unknown, would be truly "penny wise, pound foolish." Given the clear need to reduce federal spending across the board, and the decidedly mixed record of antitrust law in actually serving consumers, Congress could simply reallocate funding from the FTC's Bureau of Competition—or, more dramatically, consolidate antitrust enforcement at the DOJ and allocate the cost savings from streamlining to the FTC's Bureau of Consumer Protection.[26]

If Congress wants to improve upon the American layered approach to privacy, these suggestions offer concrete steps that could be taken today. Just as Silicon Valley's motto is "Iterate, iterate, iterate," the same approach is needed for improving our existing framework.

---

[21] Federal Trade Comm'n, FTC Operating Manual §8, *available at* http://www.ftc.gov/foia/ch08industryguidance.pdf.

[22] Federal Trade Comm'n, FTC Bureau of Consumer Protection - Resources: Guidance Documents, http://ftc.gov/bcp/menus/resources/guidance.shtm (last visited June 26, 2012).

[23] Federal Trade Comm'n, Legal Resources | BCP Business Center, http://business.ftc.gov/legal-resources/48/33 (last visited June 26, 2012).

[24] See generally, Howard Beales, III, *The FTC's Use of Unfairness Authority: Its Rise, Fall, and Resurrection*, § III, http://www.ftc.gov/speeches/beales/unfair0603.shtm [hereinafter *Beales Paper*]).

[25] *See* Szoka, *supra* at 15.

[26] See William E. Kovacic, The Institutions of Antitrust Law: How Structure Shapes Substance, 110 Mich. L. Rev. 1019, 1034 (2012) (identifying several problems with federal duality of antitrust jurisdiction).

Only by using the current framework to its fullest capacity will we actually know if there are real gaps the FTC cannot address using its existing authority. In particular, the process of issuing guidelines could identify problems as candidates for appropriately narrow legislation that could build on top of the current baseline as part of an effective layered approach—or for self-regulatory processes akin to those called for by the NTIA. If there are some forms of harm that require government intervention but that cannot fit within an appropriately limited conception of harm under unfairness, it may be better for Congress to address these through carefully tailored legislation, rather than shoehorning them into unfairness. For example, such legislation might be appropriate to prevent employers from pressuring employees into sharing their passwords to Facebook and other social networking sites.

V. The DAA: A Self-Regulatory Success Story

The Digital Advertising Alliance has demonstrated how self-regulation can evolve to provide "the flexibility, speed, and decentralization necessary to address Internet policy challenges"—not perfectly, but better than government. Since my fellow witness Bob Liodice, is representing the DAA today, let me just highlight four areas in which I think DAA has demonstrated the value of self-regulation beyond its additional principles:

- **Transparency**: In April 2010, the industry began including an icon inside targeted ads to raise awareness of the practice and offer consumers an easy opt-out from tailored advertising. That icon is now shown in over a trillion ad impressions each month.
- **Education**: Last January, DAA launched an unprecedented public awareness campaign called "Your AdChoices" to further increase public awareness of the AdChoices Icon, and consumers' ability to opt-out.
- **Evolving commitments**: In November 2011, the DAA updated its principles to bar data collected for advertising purposes from being used for employment, credit, health care treatment, or insurance eligibility decisions.[27]
- **Enforcement**: The Better Business Bureau, which administers enforcement of the DAA principles, and has done so for other self-regulatory programs since 1971, has brought a number of enforcement actions,[28] demonstrating that it is far from toothless.
- **Do Not Track**: In February, the DAA committed[29] to respect Do Not Track (DNT) headers sent by browsers when users visit websites as a (potentially) more consumer-friendly way of implementing DAA's existing privacy opt-out.

---

[27] Digital Advertising Alliance, Self-Regulatory Principles for Multi-Site Data, Nov. 2011, http://www.aboutads.info/resource/download/Multi-Site-Data-Principles.pdf.

[28] See Better Business Bureau, Case Decisions, http://www.bbb.org/us/interest-based-advertising/decisions/ (last visited June 26, 2012).

[29] Digital Advertising Alliance, DAA Position on Browser Based Choice Mechanism, Feb. 22, 2012, http://www.aboutads.info/resource/download/DAA_Commitment.pdf.

VI. Concerns about Self-Regulatory Processes

The DAA is a good example of self-regulation evolving. But not all self-regulation is created equal. I have previously outlined my concerns about the self-regulatory process the NTIA has proposed to facilitate.[30] Chief among those concerns was the role government play in steering the process through the exercise of "soft power." My participation in the World Wide Web Consortium (W3C) process as an invited expert (for the last six weeks) has increased that concern dramatically, given the looming presence of the FTC, and to a lesser extent, European governments, behind that process. In particular, I fear that an artificial deadline imposed by the FTC and other global regulators may shape the outcome of the process in ways that prove counter-productive.

More generally, despite my general skepticism of antitrust and belief that market power is best combated with market power, my experience with W3C has made me appreciate better the concerns raised by FCC Commissioner Tom Rosch about manipulation of the self-regulatory process by powerful players—especially where market power is essentially piggybacking on the soft power of government. In his dissent from the FTC's 2012 privacy report, Rosch asked: "the major browser firms' interest in developing Do Not Track mechanisms begs the question of whether and to what extent those major browser firms will act strategically and opportunistically (to use privacy to protect their own entrenched interests)."[31] And in his concurrence to the draft version of that report released in December 2010, Rosch noted: "the self-regulation that is championed in this area may constitute a way for a powerful, well-entrenched competitor to raise the bar so as to create an entry barrier to a rival that may constrain the exercise of undue power."[32]

These concerns about power are heightened by concerns about process. The W3C is highly respected as a standard-setting body, but it is not a *policy*-making body. Its first and only other policy-heavy process—to produce the Protocol for Privacy Preferences (P3P), a laudable but highly complex form of smart disclosure—was roundly criticized and never achieved widespread adoption.

Many key players are simply not represented—most notably the publishers, smaller advertising companies and data processors. All of these have a great deal to lose and could be put out of business, or forced to consolidate with larger players, in a Default DNT-On world. In large part,

---

[30] Berin Szoka, Comments to the National Telecommunications and Information Administration on the Multistakeholder Process to Develop Consumer Data Privacy Codes of Conduct, April 2, 2012, http://techfreedom.org/sites/default/files/Comments%20to%20NTIA%20on%20Self-Regulatory%20Process%204.2.12.pdf.

[31] Dissenting Statement of Commissioner J. Thomas Rosch, Issuance of Federal Trade Commission Report, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers*, Mar. 26, 2012, at 6, *available at* http://www.ftc.gov/speeches/rosch/120326privacyreport.pdf.

[32] Concurring Statement of Commissioner J. Thomas Rosch, Issuance of Preliminary FTC Staff Report, *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers*, Dec. 1, 2010, at E-3, *available at* http://www.ftc.gov/os/2010/12/101201privacyreport.pdf.

this reflects the high cost of participation, not just in terms of W3C membership,[33] but in terms of committing at least one person to engage in the weekly teleconference, the deluge of emails on the discussion list and the face-to-face meetings, which run 2.5 days.

It is also possible that the W3C Tracking Protection Working Group, while composed of talented, well-meaning and dedicated people, may simply not reflect the right mix of backgrounds, even among the companies represented. Significantly under-represented are those who could speak with authority to the real world trade-offs inherent in the many complicated decisions being made by the group—not enough business experts, no economists, and too many privacy advocates full of good intentions but lacking in real-world grounding. The stakes could scarcely be higher, with regulator standing ready to implement the outcome of the process, regardless of whether it is well-suited to the problems at hand.

Further, the process has proven highly unwieldy, given the large number of people involved and the large policy implications of the questions being debated—which were amplified considerably by Microsoft's decision to switch to Default DNT-On.

Still, for all its flaws, it may prove—to paraphrase Winston Churchill on democracy—that the W3C process is the worst possible process—except for all the others. Certainly, it is a better option than having the FTC design a DNT mechanism on its own, as has been proposed in pending legislation.[34]

I explain all these concerns in more detail below.

VII. The Dangers of Default DNT-On

Default DNT-On is supposed to empower users but in fact, it simply empowers browser makers to force a fundamental change in the Internet ecosystem, from today's low-friction, flat ecosystem of independent sites and services funded by impersonal data collection to one with fewer players who collect more data—"opt-in dystopias."

Since last September, the W3C has been developing a technical standard for Do Not Track (DNT) headers that would "allow a user to express their personal preference regarding cross-site tracking." The W3C process was based on the idea that the DNT mechanism "must reflect the user's preference." Similarly, the DAA commitment was premised on the idea that the user has "affirmatively chosen to exercise a uniform choice with the browser based tool."[35] Simply put, users, not browsers, should choose to opt-out of the data collection that creates so much value for consumers.

---

[33] A US company with over $50 million in annual revenue must pay $68,500/year, while smaller companies must pay $7900, and startups with fewer than ten employees and $3 million in annual revenue pay $2250. W3C, Membership Fees, http://www.w3.org/Consortium/fees?country=United+States&quarter=04-01&year=2012#results (last visited June 26, 2012).

[34] H.R. 654, Do Not Track Me Online Act, available at http://hdl.loc.gov/loc.uscongress/legislation.112hr654.

[35] Digital Advertising Alliance, *supra* note 27.

Microsoft breached this consensus on user choice when it announced last month that its new IE10 browser would send DNT:1 headers by default. This risks derailing the entire W3C process. Just the day before Microsoft's announcement, at the weekly W3C teleconference, privacy researcher Lauren Gelman attempted to allay industry concerns that the spec might go too far by saying: "realistically, majority default DNT is not the world this standard will exist in. DNT is going to be a 10% solution"[36]—a view overwhelmingly shared by participants.

While Microsoft's stated commitment to user empowerment is laudable, Default DNT-On doesn't empower users any more than turning on ad blocking by default would. Anyone who cares can quite easily choose to make that choice. Below a certain threshold of DNT adoption, few sites will find it worthwhile to charge, block or negotiate with those privacy-sensitive users who turn on DNT. But no-cost opt-outs and implicit *quid pro quos* don't scale: beyond a certain point, sites will have to make *quid pro quos* explicit to gain opt-ins (technically, exceptions to DNT). In other words, a significantly higher DNT adoption rate will take us past a tipping point to an opt-in world.

Some downplay the significance of this change, arguing that Default DNT-On will simply force negotiations between sites and users over granting exceptions[37]—a key part of the DNT spec. But as I explained in my comments on the draft FTC privacy report in February 2011, such negotiations are not costless; they introduce considerable transactions costs ("friction") into an ecosystem that currently works because it generated tiny amounts of value from enormous volumes of transactions. Economic theory suggests that forcing today's implicit quid pro quo to become explicit (by switching to DNT Default-On) could produce dramatically different outcomes. As I explained:

> Much as I enjoy the rich irony of seeing those who are rarely thought of as free-marketeers essentially asserting that "markets" will simply, and quickly, "figure it out," I am less sanguine. The hallmark of a true free-marketeer is not a belief that markets work perfectly; indeed, it is precisely the opposite: an understanding that "failure" occurs all the time, but that government failure is generally worse, in terms of its full consequences, than "market" failure.[38]

The first part of that lesson comes especially from the work of the economist Ronald Coase... who won his Nobel Prize for explaining that the way property rights are allocated and markets

---

[36] *See* Lauren Gelman, "Re: tracking-ISSUE-150: DNT conflicts from multiple user agents [Tracking Definitions and Compliance]", public-tracking@w3.org mailing list, May 30, 2012, http://lists.w3.org/Archives/Public/public-tracking/2012May/0341.html.

[37] Jonathan Mayer, "Do Not Track Is No Threat to Ad-Supported Businesses," Jan. 20, 2011, http://cyberlaw.stanford.edu/node/6592.

[38] Comments of Berin Szoka, on "Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers, A Preliminary FTC Staff Report of the Bureau of Consumer Protection, Federal Trade Commission, February 18, 2011, http://techfreedom.org/sites/default/files/TechFreedom%20FTC%20filing%202011-02-18.pdf

are structured determines the outcome of marketplace transactions.[39] For example, a rule that farmers bear the cost of stopping rancher's cattle from grazing on their farms by constructing fences will produce different outcomes—not merely different allocations of costs—from the opposite rule.

Coase's key insight was that, in a perfectly efficient market, the outcome would not depend upon such rules: To put this in terms of the privacy debate, the choice between, say, an opt-out rule and an opt-in rule for the collection or use of a particular kind of data (essentially a property right) would have no consequence because the parties to the transaction (say, website users and website owners) would express their "true" preferences perfectly, effortlessly and costlessly. But, of course, such frictionless nirvanas do not exist. The real world is defined by what Coase called "transactions costs": search and information costs, bargaining and decision costs, policing and enforcement costs.

The transaction costs of implementing a "Do Not Track" mechanism above an acceptable loss threshold of adoption—where sites must create architectures of negotiation—are considerable: someone must design interfaces that make it clear to the user what their choice means, the user must consume that information and make a choice about tracking, websites must decide how to respond to various possible choices and be able to respond to users in various ways through an interface that is intelligible to users, and so on—all for what might seem like a "simple" negotiation to take place.

These problems are certainly not insurmountable—and, again, with the right engineering and thoughtful user interface design a "Do Not Track" mechanism could well prove a useful tool for expressing user choice. But when we look at the world through Coase's eyes, we begin to understand how mechanism design can radically alter outcomes (in this case, funding for websites).

Put simply, Default DNT-On could take us from a world in which users can freely browse content and services offered by a thriving ecosystem of publishers to a bordered Internet. Users will either have to pay or opt-in to tracking. In this worst-case opt-in "dystopia," consumers could be made significantly worse off in three primary ways.

First, to the extent publishers have to rely on micropayments or subscriptions, their revenues will likely drop. Information goods have a marginal cost of zero, and therefore competition tends to drive their marginal cost to zero. Put more simply: unless you have a unique good protected by copyright, it's hard to charge for it (and charging for many small transactions itself creates high transactions costs). Advertising has always solved this problem by monetizing attention, but advertising online is worth three or more times more when it is tailored to users'

[39] Ronald A. Coase, The Problem of Social Cost, 3 J.L. & Econ. 1 (1960).

interests.[40] Many sites that rely on this revenue will simply disappear, or be consolidated into larger media companies. Consumers will have fewer, poorer choices.

Second, those sites and data companies that are able to obtain opt-ins will likely collect *more* data in ways that are more personal than today. While opt-ins sound great in theory, they simply do not protect privacy in the real world. As Betsy Masiello and Nicklas Lundblad explained in their seminal paper about "Opt-In Dystopias":

> opt-in regimes … are invasive and costly for the user and can encourage service providers to minimise the number of times opt-in is requested. This can have at least two adverse effects.
>
> The first is that service providers may attempt to maximise data collection in every instance that they are forced to use an opt-in framework; once a user consents to data collection, why not collect as much as possible? And the increased transaction costs associated with opt-in will lead service providers to minimise the number of times they request opt-in consent. In combination these two behaviours are likely to lead to an excessive scope for opt-in agreements. In turn, users will face more complex decisions as they decide whether or not to participate. [41]

The DNT spec allows sites to negotiate with users to grant exceptions to DNT as an explicit *quid pro quo* for access to content or services. But this could rapidly become complex given the need for users to manage exceptions for multiple sites and services:

> As this happens we are likely to see demand rise for single identity systems.... It is possible that emerging social web services could comply by setting up the opt-in as a part of the account registration process, as discussed earlier. Users have an incentive to opt-in because they want to evaluate the service; after opting-in, a user is able to make an evaluation of the service, but by that point has already completed the negotiation. The service, having already acquired the mandatory opt-in consent, has no incentive to enable users to renegotiate their choice.
>
> The data collection in this instance would all be tied to a central identity and would be likely to have excessive scope and deep use conditions. One unintended consequence of a mandatory opt-in regime might be the emergence of tethered identities, whereby a user's identity is tightly coupled with a particular social platform or service.…
>
> From a privacy point of view, tethered identities present many challenges. The concept suggests that all behaviour is tied to a single entry in a database. The

---

[40] See, Howard Beales, *The Value of Behavioral Targeting*, March 2010, http://www.networkadvertising.org/pdfs/Beales_NAI_Study.pdf.

[41] N Lundblad and B Masiello, "Opt-in Dystopias", (2010) 7:1 SCRIPTed 155, http://www.law.ed.ac.uk/ahrc/script-ed/vol7-1/lundblad.asp.

> ease of executing an overly broad law enforcement request would be far greater than in a regime of fragmented and unauthenticated data collection. The degree of behaviour upon which an advertisement might be targeted would also be far greater. And the threat of exposure posed by a security breach would also increase.

Third, few publishers and data-driven companies will be able to obtain opt-in exceptions to DNT. This will force unprecedented consolidation in the Internet ecosystem, both among publishers and among companies that use and process data for advertising, research and other purposes. As Masiello and Lundblad explain:

> A worst-case consequence of widespread opt-in models would be the balkanisation of the web. As already discussed, some degree of data collection is necessary to run many of today's leading web services. Those that require account registration, such as social web services, enjoy an easy mechanism for securing opt-in consent and would be likely to benefit disproportionately from a mandatory opt-in policy.
>
> If we believe that mandatory opt-in policies would disproportionately benefit authenticated services, we might also expect balkanisation of these services to occur. When information services are open and based on opt-out, there are incentives to provide users the best experience possible or they will take their information elsewhere. When these services are closed and based on opt-in, there are incentives to induce lock-in to prevent users from switching services. Users might be reluctant to leave a service they have evaluated and invested in; the more investment made the more likely a user is to stay with the current provider. We might expect mobility to decrease, with negative effects for competition and consumer value

Simply put, Default DNT-On is likely to drive the adoption of federated content networks, and the evolution of highly decentralized web sites and services towards an apps based model—such as on mobile phones and such as Microsoft is introducing in Windows 8—in which advertising is delivered by the app platform operator. This might or might be a good thing on net, but again, the point is that no one really knows, even as we tumble blindly down this path.

With the best of intentions, we are heading towards reshaping the fundamentals of the Internet—in ways that may have serious negative unintended consequences for privacy, the sites and services consumers enjoy, and the health of the ecosystem. But the *way* we're doing it may be even more troubling. This is not the result of a bottom-up evolutionary process, but of collusion between government and powerful market players. In the name of self-regulation, we are essentially moving toward the European model of co-regulation: where governments steer and industry rows, and where powerful incumbents use market power to serve their own agendas, with the blessing of government.

The Federal Trade Commission called for a Do Not Track mechanism in its draft privacy report, issued in December 2010. Chairman Leibowitz and David Vladeck, Director of the FTC's Bureau

of Consumer Protection, have taken credit for pressuring industry to come to the table on DNT.[42] The agency has played an active role in the W3C process. FTC Chief Technologist Ed Felten opened day two of the most recent W3C meeting by telling participants what the FTC wanted. Chairman Leibowitz and Commissioner Julie Brill delivered keynote addresses at the two prior meetings. Commissioner Brill, in particular, has pushed the W3C process to change the nature of the DNT spec to limit not just how data can be used, but what data can be collected in the first place. Representatives Ed Markey and Joe Barton have gone even further, sending a letter to the W3C Tracking Protection Working Group during its last meeting urging not only heavy restrictions on collection, but also that DNT:1 be turned on default.[43]

The FTC has clearly been turning the screws on companies to agree to comply with DNT—even before a standard exists. The FTC showed its hand in Twitter's agreement to recognize DNT in May,[44] when FTC Chief Technologist Ed Felten announced the deal himself even before Twitter could do so. Faced with the FTC's open antitrust investigation, and the agency's essentially unchecked ability to bring privacy complaints against the company, at a real cost to its reputation, it's not hard to see why Twitter might be susceptible to... encouragement from the well-meaning folks at the FTC.

So one has to wonder what role Chairman Leibowitz, and members of Congress like Representatives Barton and Markey, might have had in convincing Microsoft to break ranks from the W3C process—even if that risked derailing the process itself.

This is, of course, speculative—but not without any basis. At the very least, Congress should ask the FTC to explain exactly what its role has been throughout this process. Further, Congress should call on the agency's leadership to repudiate the disturbing argument made by Tim Wu in defense of "agency threats" as a valid form of extra-legal regulation.

VIII. Conclusion

There are no silver bullets. Neither self-regulation nor relying on Section V is without pitfalls. But together, and working in conjunction with market forces like reputation, with targeted legislative solutions, and with technological change itself, they form a layered approach to dealing with privacy that is more likely to protect us from true privacy harms without killing the goose that laid the golden egg.

---

[42] Federal Trade Commission, FTC Testifies on Do Not Track Legislation, Dec. 2, 2010, http://www.ftc.gov/opa/2010/12/dnttestimony.shtm.

[43] Letter from Congressmen Edward J. Markey and Joe Barton to World Wide Web Consortium Tracking Protection Working Group, June 19, 2012, available at http://markey.house.gov/sites/markey.house.gov/files/documents/%206-19-12%20Letter%20from%20Rep%20Markey%20and%20Barton%20-%20W3C%20.pdf.

[44] Michelle Maltais, "Twitter supports 'do not track'", Los Angeles Times, May 17, 2012, available at http://articles.latimes.com/2012/may/17/business/la-fi-tn-twitter-do-not-track-20120517.