Testimony of
Berin Szoka, President
TechFreedom[1]

on

Balancing Privacy and Innovation: Does the President's Proposal Tip the Scale?

Before the House Energy & Commerce Committee
Subcommittee on Commerce, Manufacturing, and Trade[2]
March 29, 2012

I. Introduction

The central challenge facing policymakers is three-fold:

- Defining what principles should govern privacy policy;
- Transposing those principles into concrete rules, whether through self-regulation or legislation, and updating them as technology changes; and
- Determining how to effectively enforce compliance.

Unfortunately, the privacy debate has until now focused mostly on the first part, crafting the right principles. Both President Obama's proposed "Consumer Data Privacy Framework"[3] and the FTC's Report[4] do wisely recognize not only the central importance of the second part (transposition from the abstract to the concrete), but also that the "flexibility, speed, and decentralization necessary to address Internet policy challenges"[5]—like balancing the dangers of data with its benefits—can come only from a self-regulatory process such as the Commerce Department has proposed to facilitate.[6]

---

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 COPPA before the Senate Commerce Committee on April 29, 2010, available at http://tch.fm/syexUo, ("Szoka Testimony").

2 http://energycommerce.house.gov/hearings/hearingdetail.aspx?NewsID=9404

3 The White House, Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy ("White House Report"), http://www.whitehouse.gov/sites/default/files/privacy-final.pdf.

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

5 White House Report at 23.

6 National Telecommunications and Information Administration, Request for Comments, *Multistakeholder Process to Develop Consumer Data Privacy Codes of Conduct* ("NTIA RFC"),

But both the White House and FTC propose principles that, while noble in their aspirations, may prove counter-productive for consumers if transposed without a careful consideration of the real world trade-offs inherent in regulating consumer data practices. Both documents present reformulations of the Fair Information Practice Principles. While the White House framework is perhaps the best articulation of the FIPPs thus far, the FIPPs alone cannot protect consumers effectively—at least not without imposing significant costs and burdens on consumers. The devil lies in effective transposition. As the Cato Institute's Jim Harper puts it so eloquently puts it:

> Appeals to the [FIPPs] are a ceremonial deism of sorts, boilerplate that advocates use when they don't know how to give consumers meaningful notice of information policies, when they don't know when or how consumers should exercise choice about information sharing and use, when they don't know what circumstances justify giving consumers access to data about them, and when they don't know how to describe which circumstances—much less which systems or what levels of spending—make personal data sufficiently "secure."[7]

Moreover, neither the White House nor the FTC adequately explores the legal authority and institutional capacity necessary to achieve effective enforcement, the real heat of the privacy problem. On capacity, Congress has a vital role to play in ensuring that the FTC has a clear plan to develop the in-house technical capacity it needs to keep pace with technological change and the resources needed to implement that plan.

Importantly in this regard, developing the capacity to understand and effectively regulate technology is as much about ensuring that regulators understand how innovative technology confers benefits on consumers as it is about ensuring that regulators understand how new technology *doesn't* impose imaginary costs. As technological advance brings about ever more effective means of collecting and analyzing information, there is a tendency to view this through the lense of harm—to see such advances as ever more intrusive and potentially harmful. Forty years ago, the great economist Ronald Coase warned us: "If an economist finds something—a business practice of one sort or another—that he does not understand, he looks for a monopoly explanation. And as in this field we are very ignorant, the number of understandable practices tends to be very large, and the reliance on a monopoly explanation, frequent."[8] The same risk arises here—that, finding a technology that they don't understand, regulators will look for a nefarious (or "unfair") explanation, overestimating harms to users (the more easily seen) and understating benefits (the more likely unseen).[9] Ensuring that regulators

---

https://www.federalregister.gov/articles/2012/03/05/2012-5220/multistakeholder-process-to-develop-consumer-data-privacy-codes-of-conduct.

[7] Jim Harper, *Reputation Under Regulation: The Fair Credit Reporting Act at 40 and Lessons for the Internet Privacy Debate*, Cato Policy Analysis No. 690 (Dec. 8, 2011), http://www.cato.org/pubs/pas/PA690.pdf.

[8] Ronald Coase, *Industrial Organization: A Proposal for Research*, in 3 Policy Issues and Research Opportunities in Industrial Organization, 59, 67 (Victor Fuchs ed. 1972).

[9] See Frederic Bastiat, *What Is Seen and What Is Not Seen*, http://www.econlib.org/library/Bastiat/basEss1.html

have the capacity to keep up with technological change is thus essential to facilitating both effective and appropriately restrained enforcement.

On authority, the FTC could do more with its existing unfairness authority to build a quasi-common law through enforcement actions and written guidelines on consumer data practices that cause greater consumer injury than benefit and which consumers themselves cannot reasonably avoid. The Unfairness Doctrine is a powerful tool by which the FTC can punish either practices not addressed by self-regulation or companies that simply choose not to abide by self-regulation. But it is precisely because this tool is so powerful that its use was carefully limited by the FTC in 1980—and should remain so.[10] If the Unfairness Doctrine proves too limited in the non-economic harms it recognizes, Congress should craft legislation narrowly tailored to those harms, rather than allowing the FTC to expand the scope of the Unfairness Doctrine in general. But even in legislating based on a somewhat broader conception of harm, Congress should heed the basic approach of the Unfairness Doctrine, which remains a sound basis for effective consumer protection: weigh consumer harm against consumer benefit and intervene only where consumers themselves cannot reasonably avoid the harm, such as through their own use of more effective privacy controls.

If Congress is ever to grant the FTC new authority in this area, it should at least wait to learn from the self-regulatory process. Congress should assess the failure or success of the overall self-regulatory system in three ways:

1. **Enforcement**: Can compliance with self-regulatory codes of conduct be policed effectively? If not, how can industry self-enforcement of self-regulation be strengthened? And how can FTC enforcement based on deception be enhanced?
2. **Outside Self-Regulation**: Can companies that remain outside self-regulation be policed effectively? If not, to what extent is the problem that the FTC lacks institutional capacity to use its unfairness authority effectively or that its legal authority is too limited because the limits on the Unfairness Doctrine make successful litigation too difficult?
3. **Scope & Evolution**: Does self-regulation adequately address privacy practices that, on net, harm consumers and cannot be reasonably avoided by consumers themselves?

In the first two cases, policymakers would do well to heed the paraphrase of an old adage about malice:[11] never attribute to a lack of legal authority that which can be adequately explained by a lack of institutional capacity. Of course, institutional capacity only goes as far as the FTC's legal authority, but where capacity is lacking, how can we know whether authority is really inadequate?

---

[10] FTC Policy Statement on Unfairness ("Unfairness Policy Statement"), appended to International Harvester Co., 104 F.T.C. 949, 1070 (1984). See 15 U.S.C. § 45(n).

[11] Hanlon's Razor is an eponymous adage that reads: "Never attribute to malice that which is adequately explained by stupidity." See, e.g., http://en.wikipedia.org/wiki/Hanlon's_razor.

II. A "Bill of Rights" for Consumer Privacy?

It was President Kennedy who first introduced a Consumer Bill of Rights in a speech to Congress in 1962.[12] So it is hardly unprecedented that President Obama should choose a similar label for his consumer privacy framework. No doubt this is a highly effective rhetorical framing that will drive action—whether by industry or Congress—on this complicated and often arcane topic. But the "Bill of Rights" term is problematic in two senses.

First, the Report begins and ends as constitutional sleight-of-hand. President Obama starts by reminding us of the Fourth Amendment's essential protection against "unlawful intrusion into our homes and our personal papers"—by government. But the Report recommends no reform whatsoever for outdated laws that have facilitated a dangerous expansion of electronic surveillance. In other words, while the White House embraces the "Consumer Bill of Rights" rhetoric, the *real* Bill of Rights is in peril. This was precisely the message sent by a unanimous Supreme Court two months ago in its *Jones* decision.[13] Indeed, five Justices called on Congress to remedy this situation by updating outdated laws intended to implement the Fourth Amendment's protections in digital technologies.[14] The gravest threat to our privacy comes from Congress's failure to enact such reforms—while instead focusing its limited attention on legislation mandating that private companies retain *more* information about how we use the Internet, which law enforcement could access without judicial scrutiny,[15] and cybersecurity legislation designed to facilitate the monitoring of user communications.[16] Unfortunately, the White House Report dismisses such concerns in the first footnote.[17]

Second, conceptualizing privacy in "rights" terms, while emotionally appealing, is deeply problematic. The rights contained in the *real* Bill of Rights stand between us and our government, whose proper purpose is to protect our negative rights to life, liberty and the pursuit of happiness. "Rights" are, in philosophical parlance, often conceived as "trumps" over mere "interests"—in other words, not subject to trade-offs or balancing, except perhaps with

---

[12] John F. Kennedy, 93 - Special Message to the Congress on Protecting the Consumer Interest, Mar. 15, 1962, *available at* http://www.presidency.ucsb.edu/ws/?pid=9108.

[13] U.S. v. Jones, 565 US __ (2012), http://www.supremecourt.gov/opinions/11pdf/10-1259.pdf.

[14] Id.; Berin Szoka & Charlie Kennedy, *Supremes to Congress: Bring Privacy Law Into 21st Century*, CNET, Jan. 29, 2012, http://news.cnet.com/8301-13578_3-57368025-38/supremes-to-congress-bring-privacy-law-into-21st-centur/.

[15] Berin Szoka, *Leading Free Market Groups Urge Congress to Update Key U.S. Privacy Law*, TechFreedom, April 6, 2011, http://techfreedom.org/blog/2011/04/06/leading-free-market-groups-urge-congress-update-key-us-privacy-law.

[16] Cybersecurity Act of 2012, 112th Congress (2012), http://www.hsgac.senate.gov/download/the-cybersecurity-act-of-2012-s-2105; Jim Harper, *The Senate's SOPA Counterattack?: Cybersecurity the Undoing of Privacy*, Cato@Liberty, Feb. 9, 2012, http://www.cato-at-liberty.org/the-senates-sopa-counterattack-cybersecurity-the-undoing-of-privacy/.

[17] "This framework is concerned solely with how private-sector entities handle personal data in commercial settings. A separate set of constitutional and statutory protections apply to the government's access to data that is in the possession of private parties." White House Report at 5 n. 1.

other rights.[18] This is essentially the European conception of privacy as a "fundamental human right." It conceives of privacy as a positive right, rather than the sort of negative right recognized under U.S. law. It is also essentially a property right in personal information, a problematic concept when applied to personal information.[19]

III. The Power, Risks and Benefits of Data

The privacy debate rests on a recognition of the growing power of data to shape our lives. But largely because of the conceptualization of privacy as a positive (fundamental) right, or a strict property right in personal information, the privacy debate has been systematically biased by an over-statement of the risks and an under-statement of the benefits of data. A more realistic debate would begin by weighing real privacy harms (a subject discussed below in the context of the FTC's Unfairness Doctrine) with information benefits such as:

- Enhanced advertising revenues for publishers of content and services that might otherwise have difficulty funding their offerings by charging for data, especially in markets where marginal costs are lower or zero (and basic economic theory would suggest that competition will inevitably drive prices towards zero).
- More effective advertising, which in turn means
    - More relevant, and potentially less annoying/interruptive advertising for consumers;
    - Better correlation between the production of content and services, and consumer
    - preferences;
    - Lower prices for consumers and greater innovation throughout the economy;
    - Better non-commercial messaging, too; and
    - More vibrant media and improved political discourse and communities[20]
- Serendipitous innovation based on the discovery of unexpected uses of data.

As discussed below, the FTC's existing Unfairness Doctrine provides a sound vehicle for weighing harms with benefits, and regulating only where users cannot reasonably avoid a harmful practice. But more generally, balancing risks realistic assessment of the degree to which a particular data set is likely to be tied back to a particular user at all.

---

[18] Leif Wenar, "Rights", The Stanford Encyclopedia of Philosophy (Fall 2011 Edition), Edward N. Zalta (ed.), http://plato.stanford.edu/archives/fall2011/entries/rights/#5.1.

[19] *See generally* Larry Downes, *The Laws of Disruption: Harnessing the New Forces that Govern Life and Business in the Digital Age* 70-71 (2009).

[20] *See generally* Berin Szoka, *Privacy Trade-Offs: How Further Regulation Could Diminish Consumer Choice, Raise Prices, Quash Digital Innovation & Curtail Free Speech,* Comments the FTC Privacy Roundtables (Dec. 7, 2009), *available at* http://www.ftc.gov/os/comments/privacyroundtable/544506-00035.pdf

IV. PII, Anonymization & Re-Identification

The FTC's 2010 Preliminary Staff Report hinted that the agency might abandon the traditional distinction between PII and non-PII on the grounds that relevance of this distinction is decreasing as it becomes possible to identify anonymous datasets, or to re-identify de-identified data.[21] But in the face of criticism, the final FTC Report changed course and clarified that "data is not 'reasonably linkable' to the extent that a company: (1) takes reasonable measures to ensure that the data is de-identified; (2) publicly commits not to try to re-identify the data; and (3) contractually prohibits downstream recipients from trying to re-identify the data." This is an eminently sensible compromise.

While the White House Report does not explicitly address the debate that has raged behind this reversal of positions, nor does it emphasize the importance of de-identification in general, it does specifically call for de-identification as a core element of its "Transparency"[22] and "Focused Collection"[23] principles.[24]

Ensuring proper de-identification should be a core goal of self-regulation—and legislation, if that proves necessary. Balancing realistic risks of re-identification with a realistic assessment of harms likely to flow from re-identification is essential to ensuring that privacy regulation (and self-regulation) benefits consumers. As Brooklyn Law School professor Jane Yakowitz explains in her seminal 2011 law review article, Tragedy of the Data Commons:

> Accurate data is vital to enlightened research and policymaking, particularly publicly available data that are redacted to protect the identity of individuals. Legal academics, however, are campaigning against data anonymization as a means to protect privacy, contending that wealth of information available on the Internet enables malfeasors to reverse-engineer the data and identify individuals within them. Privacy scholars advocate for new legal restrictions on the collection and dissemination of research data. This Article challenges the dominant wisdom, arguing that properly de-identified data is not only safe, but of extraordinary social utility. It makes three core claims. First, legal scholars have misinterpreted the relevant literature from computer science and statistics, and thus have significantly overstated the futility of anonymizing data. Second, the available evidence demonstrates that the risks from anonymized data are theoretical - they rarely, if ever, materialize. Finally, anonymized data is crucial to

---

[21] FTC 2010 Report at 39.

[22] "[C]ompanies should provide clear descriptions of what personal data they collect, why they need the data, how they will use it, when they will delete the data or *de-identify it from consumers*, and whether and for what purposes they may share personal data with third parties." White House Report at 14 (emphasis added).

[23] "Companies should securely dispose of or *de-identify personal data once they no longer need it*, unless they are under a legal obligation to do otherwise." White House Report at 21 (emphasis added).

[24] The Report also notes that the Department of Health and Human Services "plans to issue additional guidance on the HIPAA Privacy Rule's "minimum necessary" standard and on de-identification of health information under the HIPAA Privacy Rule. White House Report at 43.

> beneficial social research, and constitutes a public resource - a commons - under threat of depletion. The Article concludes with a radical proposal: since current privacy policies overtax valuable research without reducing any realistic risks, law should provide a safe harbor for the dissemination of research data.[25]

V. Individual Control

The White House's first principle is that "Consumers have a right to exercise control over what personal data companies collect from them and how they use it." This is probably the most viscerally compelling principle[26] but is deeply problematic if understood as a "right" to be strictly enforced rather than an aspirational principle to be transposed pragmatically, depending on the trade-offs inherent in the real world. Hence, the vital importance of the word "appropriate."

The concept has its roots in the original 1890 law review article by Warren and Brandeis that gave birth to modern privacy law, where they declared that:

> Recent inventions & business methods call attention to... the right "to be let alone." Instantaneous photographs & newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that "what is whispered in the closet shall be proclaimed from the house-tops.'"[27]

By contrast, the Supreme Court ruled in 1967 that:

> Exposure of the self to others in varying degrees is a concomitant of life in a civilized community. The risk of this exposure is an essential incident of life in a society which places a primary value on freedom of speech and of press.[28]

In other words, much as we might want a right to keep people from speaking about us, we do not have, as the White House Report suggests if read literally, "a right to exercise [*absolute*] control over what personal data companies collect from [us] and how they use it."[29] UCLA Law professor Eugene Volokh explained this best in his seminal 2000 law review article, "Freedom of Speech, Information Privacy, and the Troubling Implications of a Right to Stop People from Speaking About You.":

---

[25] Jane Yakowitz, *Tragedy of the Data Commons*, 25 Harv. J. of Law & Tech 1 (Fall 2011), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1789749.

[26] "Properly defined, privacy is the subjective condition people experience when they have power to control information about themselves." Jim Harper, Cato Institute, Understanding Privacy – and the Real Threats to It, Cato Institute Policy Analysis No. 520, Aug. 4, 2004, http://www.cato.org/pub_display.php?pub_id=1652.

[27] Warren & Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193 (Dec. 15, 1890), *available at* http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html.

[28] Time, Inc. v. Hill, 385 U.S. 374, 388 (1967).

[29] White House Report at 1.

> Government attempts to let us "control … information about ourselves" sound equally good: Who wouldn't want extra control, especially of things that are by hypothesis personal? And what fair-minded person could oppose requirements of "fair information practices"?
>
> The difficulty is that the right to information privacy—the right to control other people's communication of personally identifiable information about you—is a right to have the government stop people from speaking about you. We already have a code of "fair information practices," and it is the First Amendment, which generally bars the government from "control[ling the communication] of information" (either by direct regulation or through the authorization of private lawsuits, whether the communication is "fair" or not. While privacy protection secured by contract turns out to be constitutionally sound, broader information privacy rules are not easily defensible under existing free speech law.[30]

There are also real costs to choice, and benefits of having no choice, as Indiana University Law professor Fred Cate argues in his essay, "The Failure of Fair Information Practice Principles":

> In some cases, consent may be undesirable, as well as impractical. This is true of press coverage of public figures and events, medical research, and of the many valuable uses of personal information where the benefit is derived from the fact that the consumer has not had control over the information. This is certainly true of credit information: its value derives from the fact that the information is obtained routinely, over time, from sources other than the consumer. Allowing the consumer to block use of unfavorable information would make the credit report useless.[31]

These practical and constitutional realities are already recognized by U.S. privacy law. The Fair Credit Reporting Act, for example, does not allow us to control what others say about our credit history, but instead gives us access and correction rights to make sure the information on which they base what they say about us is accurate.[32] This is premised not on our ownership of "our" information, but on the clear harms that can follow from inaccurate speech about us. While the FCRA is far from perfect,[33] it is at least an example of how a harms-based approach can serve as the basis for preventing harmful uses of information about us. And this example illustrates that even a principle as appealing as individual control cannot be treated as a "right" but must be transposed carefully to apply to a particular privacy problem.

---

[30] Eugene Volokh, *Freedom of Speech, Information Privacy, and the Troubling Implications of a Right to Stop People from Speaking About You*, 1999, *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=200469.

[31] Fred H. Cate, *The Failure of Fair Information Practice Principles*, 2006, *available at* http://ssrn.com/abstract=1156972.

[32] Fair Credit Reporting Act (FCRA), 15 U.S.C. § 1681 et seq., *available at* http://www.ftc.gov/os/statutes/031224fcra.pdf.

[33] Harper, *Reputation Under Regulation, supra* note 7.

VI. Transparency

In some ways, the transparency principle is perhaps universally embraced in the White House Report. While many questions remain over whether we can rely on notice of a company's privacy practices, and some, like Fred Cate note the costs and failures of notice,[34] it does remain a sound aspirational principle that must be transposed effectively.

The main shortcoming of this principle is that it contemplates that the work of notice will be done primarily, if not entirely, by "plain language statements about personal data collection, use, disclosure, and retention." While such statements *are* important and should be made more readable and conspicuous where feasible, as the FTC Report also proposes,[35] they should be supplemented in two key ways.

First, companies should be encouraged to educate consumers through more accessible forms of notice that explain privacy policies and practices, as the FTC Report contemplates. This could include short videos such as on Google's Privacy Channel on YouTube,[36] FAQs, just-in-time notices about how mobile apps collect data, and so on. The FTC should be commended for making this general inquiry the focus of its upcoming May Workshop.[37]

Second, the White House missed an opportunity to promote the concept of "Smart Disclosure" developed by Cass Sunstein, director of the Office of Information and Regulatory Affairs, a close advisor to the President, and a widely respected thinker in law, policy and technology. In an OIRA memo to agency heads issued last fall, Sunstein defined "smart disclosure" as:

> the timely release of complex information and data in standardized, machine readable formats in ways that enable consumers to make informed decisions. Smart disclosure will typically take the form of providing individual consumers of goods and services with direct access to relevant information and data sets. Such information might involve, for example, the range of costs associated with various products and services, including costs that might not otherwise be transparent. … In many cases, smart disclosure enables third parties to analyze, repackage, and reuse information to build tools that help individual consumers to make more informed choices in the marketplace.

This provides a powerful vision for reconceiving transparency as something that can be technologically intermediated—meaning that a company's disclosure of its privacy practices (among other things) need no longer be limited to the simplified form of its plain language

---

[34] "Businesses and other data users are burdened with legal obligations while individuals endure an onslaught of notices and opportunities for often limited choice. Notices are frequently meaningless because individuals do not see them or choose to ignore them, they are written in either vague or overly technical language, or they present no meaningful opportunity for individual choice." Cate, *supra* note 31, at 1.

[35] FTC Report at 61.

[36] The Google Privacy Channel, YouTube, http://www.youtube.com/googleprivacy

[37] Press Release, Federal Trade Commission, FTC Will Host Public Workshop to Explore Advertising Disclosures in Online and Mobile Media on May 30, 2012, Feb. 29, 2012, http://www.ftc.gov/opa/2012/02/dotcom.shtm.

disclosure (though, as discussed below, they should be consistent, or punished under the FTC's deception authority). Meaningful smart disclosure on privacy could bypass much of the current debate about the failure of effective notice to empower consumers by making "notice" technologically actionable: 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..

Further, as the FTC Report notes, "Machine-readable policies, icons, and other alternative forms of providing notice also show promise as tools to give consumers the ability to compare privacy practices among different companies."[38] Again, the example of 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.

The FTC Report contemplates a particular application that as Commissioner Brill put it in a public response to my question at a Direct Marketing Association event on the day the FTC Report was released, "... is the first step towards structured disclosure more generally."[39] Specifically, the FTC Report proposes that:

> the data broker industry explore the idea of creating a centralized website where data brokers that compile and sell data for marketing could identify themselves to consumers and describe how they collect consumer data and disclose the types of companies to which they sell the information. Additionally, data brokers could use the website to explain the access rights and other choices they offer consumers, and could offer links to their own sites where consumers could exercise such options. This website will improve transparency and give consumers control over the data practices of companies that maintain and share data about them for marketing purposes.[40]

This concept merits exploration as a way of remedying the lack of transparency regarding companies that currently lack a direct way of offering transparency to those whose data they collect—provided the term "data broker" is defined appropriately. This could be an excellent test case for encouraging smart disclosure through self-regulation—but only if it can be implemented in a way that actually improves transparency for consumers and proves feasible for companies.

---

[38] FTC Report at 62.

[39] Keynote Address by FTC Commissioner Julie Brill at DMA in DC 2012, March 26, 2012, http://newdma.org/dma-in-dc

[40] FTC Report at 69.

VII. Transposition of Principles

Setting aside the first question raised at the outset (choosing the right principles), the core problem remains a practical one: How to translate a set of principles (or "rights") into workable guidelines and, where appropriate, binding rules that inform how data flows across the Internet through countless interactions every minute and through technologies yet to be conceived.

The Report aptly summarizes the virtues of "open, transparent multistakeholder processes": "when appropriately structured, they can provide the flexibility, speed, and decentralization necessary to address Internet policy challenges."[41] American reliance on multistakeholder processes has, as the Report notes, allowed the U.S. Internet policy to avoid "fragmented, prescriptive, and unpredictable rules that frustrate innovation and undermine consumer trust."[42] (This essentially affirms what the FTC said in its 1999 report on privacy: "[S]elf-regulation is the least intrusive and most efficient means to ensure fair information practices, given the rapidly evolving nature of the Internet and computer technology."[43])

But just as the value of privacy principles depends on their transposition into real-world guidelines, that process of transposition depends on whether it is "appropriately structured."[44] In both cases, what matters is not the intention, but the process, for the process is what determines the outcome. If we wish to avoid "failure by design," we must take care to answer the following critical questions carefully.

First, what role will government play? The White House Report says, "The Federal Government will work with stakeholders to establish operating procedures for an open, transparent process. Ultimately, however, the stakeholders themselves will control the process and its results."[45] Fulfilling this promise requires that, if government officials actually serve as facilitators for the process, they must remain neutral conveners, and the principles contained in the White House Report must be clearly understood as one set of hortatory principles, rather than criteria by which the success of the self-regulatory process *must* be judged.

This is the most important factor separating the kind of self-regulation praised by the White House and what the Europeans call "co-regulation." In self-regulation, government may suggest aspirational principles (as the White House has done) and play a convening role, but in co-regulation, government "steers while industry rows," steering the process to determine its outcome. Co-regulation is, in fact, just another vehicle for governmental regulation; and while it might seem comfortably familiar to European privacy regulators, it cannot be relied on to deliver the workable policy framework that can only be forged in a true self-regulatory process as a voluntarily agreed upon compromise among many stakeholders with conflicting interests.

---

41 *Id*. at 23.

42 *Id*. at 24.

43 1999 FTC Report at 6.

44 White House Report at 24.

45 *Id*. at 24.

While the experience of the Digital Advertising Alliance,[46] for example, is a great example of how a multi-stakeholder process can achieve industry consensus on a difficult set of issues, it verges on co-regulation in one key respect: This process is not a high-level framework such as that proposed by the White House Report, but a sector-specific set of principles for online behavioral advertising developed by the FTC.[47] However admirable the end result, the more specifically government sets the basic contours of the self-regulatory process, the more likely that process is to produce outcomes that prove unworkable to some in industry.

Indeed, the less the multistakeholder process verges on co-regulation, the lower the risk of another failure point in the self-regulatory process: a legal challenge by a company that the process constituted government action that should have been subject to normal rulemaking requirements, or that it exceeded the jurisdiction of whichever agency might run the process.

Second, just how "open" and "transparent" must the process be? Requiring all discussions to take place in public would chill the very open dialogue among companies about their technologies and business practices necessary to allow self-regulation to distill widely dispersed expertise into workable compromises. This reality demands that at least some negotiations be conducted in private, without government or privacy advocates in the room—because both could use information derived from these negotiations in litigation against (or at least public criticism of) particular companies, something that would chill candid participation by those companies.

Third, how will civil society groups participate in the process? If they may exercise a "heckler's veto," they could derail the process. On the other hand, they may prove invaluable to the success of the process so long as their criticism is constructive, offering concrete suggestions on how to better protect privacy. And to the extent they can support the codes of conduct that result from the process, or at least the legitimacy of the process that produced them, the evolving U.S. privacy regime will benefit from greater acceptance by the public and our International partners. Of course, they need not accept these codes as the final word on the matter, and remain free to produce their own "minority report" or lobby for legislation in a particular area.

The model of the Digital Advertising Alliance is thus further instructive: Industry responded to the problem identified by the FTC's 2009 “Self-Regulatory Principles For Online Behavioral Advertising” by convening their own multi-stakeholder process behind closed doors, resulting in a set of principles unanimously approved by the participating companies.[48] The DAA published a draft report, solicited feedback from privacy advocates and the FTC, and reconvened their process to produce a final code of conduct, to which they unanimously certified.

---

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

[47] Federal Trade Commission, *Self-Regulatory Principles for Online Behavioral Advertising* (2009), http://www.ftc.gov/os/2009/02/P085400behavadreport.pdf.

[48] Digital Advertising Alliance, *Self-Regulatory Principles for Online Behavioral Advertising* (2009), http://www.aboutads.info/resource/download/seven-principles-07-01-09.pdf.

Fourth, by whom will self-regulatory codes of conduct be subject to approval? The White House Report merely says "the stakeholders themselves will control the process and its results"[49] but does not clarify what that means. Outrageous as it will surely seem to some, it must be industry itself that determines whether to approve a code of conduct. Otherwise, the process will fail because companies simply will not abide by the codes of conduct it produces. This is likely to be the most controversial aspect of designing the multi-stakeholder process because the expectations of privacy advocates are simply unrealistic. For example, in testimony before this Subcommittee last October, Pam Dixon of the World Privacy Forum demanded "Consumer, public interest and other independent representatives must be fully represented (if possible, up to 75 percent or more) on the governing bodies of self-regulatory schemes."[50]

Given such expectations, not getting to vote *at all* on approval will be a difficult pill for many well-meaning privacy advocates to swallow. But they can still meaningfully shape the outcome of these self-regulatory processes even without voting on the final product, not only through their official input in the process, but through their ability to channel public pressure on the companies that participate. The widespread public opposition to SOPA and PIPA earlier this year demonstrated just how powerful public pressure can be. There is no reason why civil society groups cannot attempt to use such grassroots pressure to influence the self-regulatory process.

Fifth, regardless of *who* votes, what will be the mechanism for voting? How high will the threshold be for approval, and how will voting power be determined? These are questions best answered by professionals with expertise in designing choice mechanisms for multi-stakeholder processes. As a number of economists have shown, the outcomes of a voting system are highly contingent on its structure.[51] Commissioner Rosch's concern about the danger of capture by industry leaders is worth noting.[52] But it nonetheless seems inevitable that voting power will have to be related in some fashion to market share. Otherwise, the outcome will be determined by who can get more seats at the table—much as the Soviet Union once tried to increase its representation in the United Nations by insisting that Soviet Republics like Byelorussia and Ukraine deserved their own seats.[53]

---

[49] White House Report at 24.

[50] Testimony of Pam Dixon, Executive Director, World Privacy Forum, Before the Subcommittee on Commerce, Manufacturing, and Trade of the House Committee on Energy and Commerce, Oct. 13, 2011, at 11, http://republicans.energycommerce.house.gov/Media/file/Hearings/CMT/101311/Dixon.pdf.

[51] James Buchanan & Gordon Tullock, *The Calculus of Consent: Logical Foundations of Constitutional Democracy*, http://www.econlib.org/library/Buchanan/buchCv3.html.

[52] "[T]he 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. That possibility may be blunted by insuring that smaller rivals participate in the adoption of self-regulatory rules, but that may not be practical." Rosch statement, 2010 Draft Privacy Report at E-3.

[53] *See* N.S. Timasheff, *Legal Aspects of the Grant of Three Seats to Russia in the United Nations Charter*, 14 Fordham L. Rev. 180 (1945), http://ir.lawnet.fordham.edu/flr/vol14/iss2/4.

Sixth, will there be a shot clock for the process? If so, how will it work? If not, how can we ensure that each self-regulatory process work expeditiously and that those companies that prove resistant to compromise will not unduly drag out the process as a negotiating tactic? As with the voting mechanism, reasonable time limitations that are made clearly *ex ante* can help to avoid process failure—so long as they provide adequate time to resolve the issues specific to that process.

Seventh, how will the initial selection of issues work? The White House Report proposes only that "Stakeholder groups, with the assistance of NTIA, will identify markets and industry sectors that involve significant consumer data privacy issues and may be ripe for an enforceable code of conduct."[54] This conversation is probably one that can happen entirely in public, and would very much benefit from the active (and constructive) participation of civil society groups. The best way to approach this process may be to create a prioritized list of issues that make sense of the basis for a potential code of conduct, either specific to an industry or to a cluster of related practices.

For example, early topics to be considered might include transparency in the mobile ecosystem (a topic on which the FTC will hold a workshop in May[55]), cross-border transfers of cloud data, and transparency regarding "data brokers" whose operations are not directly visible to the public (a topic identified as critical by the FTC Report—but without any definition of the broad term "data broker"[56]). Other topics that may merit attention include the portability of user data, interoperability of privacy controls, and machine-readable disclosures (discussed above).

Finally, how exactly will self-regulatory codes of conduct be updated? By shaping expectations during initial negotiation, this question will play a large role in the success or failure of the initial process. The White House Report raises as many questions as it answers in this regard with its discussion of "evolution": "Stakeholders may decide at any time that a code of conduct no longer provides effective consumer data privacy protections, in light of technological or market changes."[57] How many? Much like the initial voting mechanism question, industry participants need to know *ex ante* what will be required to re-open negotiation of, and actually amend, a code of conduct. This is probably a question best resolved by industry itself in the initial negotiations. "NTIA might also … seek to re-convene stakeholders. As with the initial development of a code of conduct, however, stakeholder participation in the process to revise a code of conduct would be voluntary."[58] So what will constitute an effective "quorum" for a revised process? Or will it be sufficient that some companies might accede to a version 2.0 of a code? What will happen if a code "forks" into multiple pieces (as sometimes happens with

---

[54] White House Report at 26.

[55] Press Release, Federal Trade Commission, FTC Will Host Public Workshop to Explore Advertising Disclosures in Online and Mobile Media on May 30, 2012, Feb. 29, 2012, http://www.ftc.gov/opa/2012/02/dotcom.shtm.

[56] FTC Staff Report at 68-70.

[57] White House Report at 27.

[58] *Id.*

open source standards)? If "Congress could prescribe a renewal period for codes of conduct," what would be required to renew and extend them?

VIII. Accountability: Effective Enforcement

Having discussed the first and second questions identified at the start of this testimony, let us now turn to the third: how the FTC can effectively enforce compliance. This has three component parts:

- Institutional enforcement capacity
- Deception authority
- Unfairness authority

The White House Report rightly emphasizes the need for "strong enforcement," but focuses on granting new legal authority to the FTC. Before reaching this point, the Report should have asked whether the FTC has the enforcement capacity necessary to use its existing authority—or to use any new authority it might be given—and whether that existing legal authority is being fully realized.

A. Enforcement by the Reputation Market

But before turning to turning enforcement by government, it is worth considering the way the Internet itself facilitates pressure on companies through the "reputation market" to abide by their privacy promises and improve their privacy practices. 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 to 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 its "What They Know" series,[59] which has been popularized using social media tools.

Social media tools were recently used to great effect to express grassroots concern about proposed copyright legislation. While some Internet companies certainly helped to promote these messages, even without their involvement, this experience demonstrates 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.[60] Among the most important factors driving companies to participate

---

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

[60] 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 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.").

constructively in the multi-stakeholder process, to forge meaningful privacy protections, and to abide by them will be the fear of a Wall Street Journal article, a social media frenzy, or organized campaign demanding action on a particular privacy problem.

B. Enhancing the FTC's Institutional Technical Capacity

Effective FTC enforcement requires the technical knowledge of the industry. Chairman Leibowitz deserves credit for appointing the agency's first Chief Technologist.[61] But even with someone as talented as Ed Felten in that position, the FTC is still way behind the curve: Ed's title is not Chief Technology *Officer* because there is no office behind him. Just over five years ago, Peter Swire called on the agency to "consider a new office of information technology to assist the Commission in making effective decisions about how to protect consumers in Internet activities. This office would parallel the FTC's in-house capability in economics, and would permit the FTC to act strategically to protect consumers from emerging online threats."[62]

Specifically, the Report should have called for 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.

These suggestions in no way diminish the important enforcement work done by the FTC's hardworking staff. To the contrary, it is unfair and unrealistic to expect the FTC to fulfill its consumer protection mission in the face of massive technological change without the expertise required to stay ahead of that change. If, in the last five years, policymakers had spent a fraction as much time on improving the FTC's institutional capacity as inventing new authority, the U.S. privacy regime would be far more effective in protecting consumers and ensuring their trust, and less easily dismissed as inadequate by foreign privacy regulators.

C. Enhancing the FTC's Deception Authority through Smart Disclosure

Punishing deception is the bedrock of the FTC's current privacy regime[63]—and it will the the ultimate tool for ensuring accountability by companies to the self-regulatory codes of conduct to which they subject themselves. Yet both the White House Report and the FTC Report miss

---

[61] Federal Trade Commission, *FTC Names Edward W. Felten as Agency's Chief Technologist; Eileen Harrington as Executive Director*, Nov. 4, 2010, http://www.ftc.gov/opa/2010/11/cted.shtm.

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

[63] "[T]he Commission will find deception if there is a representation, omission or practice that is likely to mislead the consumer acting reasonably in the circumstances, to the consumer's detriment." FTC Policy Statement on Deception, 1983, http://www.ftc.gov/bcp/policystmt/ad-decept.htm (appended to Cliffdale Associates, Inc., 103 F.T.C. 110, 174 (1984)).

an important opportunity to enhance the FTC's deception authority through the enforcement of structured, machine-readable disclosures.

At a minimum, such disclosures could be used to indicate which self-regulatory codes of conduct the site or service complies with. This, in turn, should facilitate FTC enforcement by allowing the agency to easily determine the universe of companies acceding to the code.

In a more robust form, machine-readable disclosures could also be used by companies that want to accede to most of a code of conduct but not to particular components of its rules—or all of a code, *plus* additional protections. This might create a practicable way of managing enforcement of a multiplicity of codes of conduct without requiring binary all-or-nothing compliance. That, in turn, might help to facilitate both successful resolution of the multistakeholder process and continuing competition on privacy. In other words, companies are more likely to treat codes of conduct as a floor for their practices, rather than a ceiling, if they can be rewarded for exceeding the basic requirement of a code.

But to succeed in promoting the White House's Accountability principle, smart disclosures must be as legally enforceable as the plain language versions to which they correspond. The Deception Doctrine requires that a misrepresentation or omission be both likely to mislead a consumer and "material."[64] Thus, for example, a machine-readable statement about corporate privacy practices that was implemented as an industry standard but never adopted in any way that consumers actually relied upon might not be subject to a deception action, no matter how misleading a disclosure in that format might be. On the other hand, once relied upon by even a relatively small group of consumers, such a disclosure system *should* be legally enforceable under the Deception Policy Statement, which specifically notes that, "If the representation or practice affects or is directed primarily to a particular group, the Commission examines reasonableness from the perspective of that group."[65] In other words, even if only a relatively niche group of "power users" used a setting in their app store to limit installations to apps that complied with certain privacy practices, or acceded to particular codes, these representations should be enforceable by the FTC.

Unfortunately, such case of widespread deception has persisted for many years without an FTC enforcement action. In 2002, W3C published P3P: The Platform for Privacy Preferences,[66] which allows websites to describe their privacy practices in a compact privacy policy. Internet Explorer, starting with version 6 (released in 2001), will, by default, not load third party cookies from sites that do not have a compact privacy policy.[67] It was widely known for many years that many companies created compact privacy policies that did not correspond to their human-readable privacy policy (or their actual privacy practices), but in 2008 Lorrie Faith Cranor

---

64 *Id.*

65 *Id.*

66 Platform for Privacy Preferences (P3P) Project, Enabling Smarter Privacy Tools for the Web (2007), http://www.w3.org/P3P/.

67 Privacy in Microsoft Internet Explorer 6, MSDN, http://msdn.microsoft.com/en-us/library/ms537343.aspx

published a research paper documenting widespread mis-statements in P3P policies.[68] In December, a federal court dismissed a suit against Amazon on similar grounds for lack of standing,[69] making it clear that if P3P policies are to be enforced, the task must fall to the FTC.

While the FTC has never, to my knowledge, explained why it has not brought an enforcement case based on P3P misrepresentations, one possible explanation is that they have concluded that the IE6 implementation is inadequate to demonstrate that the representations within the compact privacy actually mislead consumers, as the Deception Policy Statement requires, because IE6 requires only that a site have a policy, not that the policy say anything in particular.

If so, the lesson is that any self-regulatory effort geared toward using machine-readable disclosures should be conducted in conjunction with those who might develop tools based on such disclosures, particularly browser-makers, to ensure that the useful disclosures are implemented by useful tools.

D. Using the FTC's Unfairness Authority

The FTC's unfairness jurisdiction is often mentioned only as an afterthought, but in fact, as the Commission has held, "unfairness is the set of general principles of which deception is a particularly well-established and streamlined subset."[70] As so often happens in policy discussions, the Report pays scant attention to the FTC's unfairness jurisdiction, merely noting, in a footnote, that it "will remain an important source of consumer data privacy protection."[71] In fact, this jurisdiction is the key to how the FTC could effectively police online privacy outside of self-regulation—punishing companies that do not participate in self-regulation as well as practices that are not prohibited by self-regulation.

This jurisdiction is a powerful tool against privacy abuses because it allows the FTC to build a quasi-common law limiting harmful trade practices as technology evolves. But unfairness can

---

[68] Lorrie Faith Cranor, Serge Egelman, Steve Sheng, Aleecia M. McDonald & Abdur Chowdhury, *P3P Deployment on Websites*, 7 Electronic Commerce Research and Applications 3, 274-293 (Autumn 2008), *pre-print available at* http://lorrie.cranor.org/pubs/p3p-deployment.html (In a study comparing the actual P3P policies of 21 popular websites to the corresponding natural language policies, the researchers found that only two P3P policies correctly specified the types of data that were being collected. As a result, "users reading only a P3P policy might be surprised to find a site collecting more data than what was advertised." p. 40. All of the sites has discrepancies regarding the ways in which collected data may be used. p. 40-41. And "[o]nly six of the websites examined either accurately report their data sharing policies ... or their P3P policies are overly inclusive ... in their reporting of data sharing." p. 41.).

[69] Del Vecchio v. Amazon, C11-366-RSL (W.D. Wash.; Dec. 1, 2011), available at http://docs.justia.com/cases/federal/district-courts/washington/wawdce/2:2011cv00366/174037/58/0.pdf?ts=1322842930; *see also* Venkat Balasubramani, *The Cookie Crumbles for Amazon Privacy Plaintiffs – Del Vecchio v. Amazon*, Technology & Marketing L. Blog, Dec. 2, 2011, http://blog.ericgoldman.org/archives/2011/12/the_cookie_crum.htm.

[70] International Harvester, 104 F.T.C. 949, 1060 (1984) *(cited in* J. 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*]).

[71] Report at 27 note 32.

be a dangerous legal weapon if unleashed from its current limitations. Understanding the checkered history of the Unfairness Doctrine is essential to understanding the evolution of the FTC and U.S. consumer protection law more generally. In brief, until 1964, the agency generally did not distinguish between unfair acts and deceptive ones. In 1964, the agency defined "unfairness" in highly subjective terms, without weighing the benefits of a practice or how easily consumers could avoid it.[72] This led the FTC on an unfairness rule-making spree, trying to regulate everything from funeral home practices to advertising to children—to the point that it was dubbed the "National Nanny" by the Washington Post—hardly a Thatcherite bastion.[73] In fact, the Democratic Congress responded by briefly shutting down the agency and slashing its budget to make it clear that it had not dubbed the agency a regulatory knight errant, free to tilt its steely lance at imagined windmills of "unfairness" or "deception."[74] While this experience did serious harm to the FTC's institutional capacity,[75] it also led to the formulation of clear policy statements on unfairness (in 1980) and deception (in 1983), both at the request of Congress. These today provide the basis for the FTC's enforcement actions, and also reasonably clear legal standards by which companies may predict their legal liability. In 1994, Congress enshrined the Unfairness Policy Statement in the FTC Act itself.[76]

Under the Statement and the 1994 amendment, the Commission applies a two part test. First, it asks whether an "unjustified consumer injury" has occurred:

> To justify a finding of unfairness the injury must satisfy three tests. It must be substantial; it must not be outweighed by any countervailing benefits to consumers or competition that the practice produces; and it must be an injury that consumers themselves could not reasonably have avoided.[77]

Second, the FTC will consider:

> whether the conduct violates public policy as it has been established by statute, common law, industry practice, or otherwise. This criterion may be applied in two different ways. It may be used to test the validity and strength of the

---

[72] See generally, Beales Paper, *supra* note 70.

[73] *Id.* (*citing* Wash. Post, March 1, 1978).

[74] *Id*.

[75] The agency in 2010 had 34% fewer full time equivalent employees as it did in 1980 (even without adjusting to for the growth in U.S. population)—and that number has grown significantly since the original slashing. *See* FTC Full-Time Equivalent History, http://www.ftc.gov/ftc/oed/fmo/fte2.shtm.

[76] 15 U.S.C. § 45(n) ("The Commission shall have no authority under this section or section 57a of this title to declare unlawful an act or practice on the grounds that such act or practice is unfair unless the act or practice causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.").

[77] 1980 FTC Unfairness Policy Statement.

> evidence of consumer injury, or, less often, it may be cited for a dispositive legislative or judicial determination that such injury is present.[78]

But, by statute, "[s]uch public policy considerations may not serve as a primary basis for such determination."[79] Howard Beales has summarized the Unfairness Doctrine as follows:

> the modern unfairness test reflects several common sense principles about the appropriate role for the Commission in the marketplace. First, the Commission's role is to promote consumer choices, not second-guess those choices. That's the point of the reasonable avoidance test. Second, the Commission should not be in the business of trying to second guess market outcomes when the benefits and costs of a policy are very closely balanced or when the existence of consumer injury is itself disputed. That's the point of the substantial injury test. And the Commission should not be in the business of making essentially political choices about which public policies it wants to pursue. That is the point of codifying the limited role of public policy.[80]

The FTC has used its unfairness authority to protect privacy in several lines of cases. First, as noted in the FTC's 2010 Preliminary Staff Report, the Commission brought a number of unfairness cases requiring adequate security practices.[81] But as Commissioner Rosch noted in his concurring statement, "there was financial harm threatened in those cases."[82] Second, the FTC has brought unfairness actions to punish retroactive application of a revised privacy policy.[83] Third, late last year, the FTC brought, and successfully settled (but did not fully litigate) an unfairness case against Frostwire, the maker of a mobile peer-to-peer file-sharing program for its unfair product design. This case is groundbreaking both because it applies unfairness in the context of how product design can cause users to share more information than they expect and because it rests on non-monetary harms.

E. Unfairness and the Harm Debate

As noted above, the extent of the Unfairness Doctrine's applicability rests primarily on how broadly harm is defined—as is implied by the FTC's declaration that "Unjustified consumer injury is the primary focus of the FTC Act.""[84]

---

[78] *Id.*

[79] 15 U.S.C. § 45(n).

[80] Beales Paper, *supra* note 70.

[81] 2010 FTC Report at 10.

[82] 2010 FTC Report at E-2 n. 3.

[83] See, e.g., Gateway Learning Corp., No. C-4120, 2004 WL 2618647 (F.T.C. Sept. 10, 2004), *available at* http://www.ftc.gov/os/caselist/0423047/0423047.shtm; Federal Trade Commission, *Self-Regulatory Principles for Online Behavioral Advertising supra* note 47, at 19; *see also* In re Orkin Exterminating Co., 108 F.T.C. 263 (1986), aff'd, 849 F.2d 1354 (11th Cir.).

[84] 1983 FTC Unfairness Policy Statement.

Even critics of the Unfairness Doctrine have been careful not to rule out its proper application in privacy cases. For example, in 2000, the Commission settled an enforcement action against ReverseAuction, which had violated eBay's terms of service by "using the e-mail addresses, eBay user IDs, and feedback ratings of eBay registered users for the purposes of sending unsolicited commercial e-mail to such registered eBay users."[85] Commissioners Swindell & Leary dissented, in part, on the grounds that this should have been a pure deception case and that violating user privacy by sending such unsolicited email "did not cause substantial enough injury to meet the statutory standard" but emphasized that "[w]e do not say that privacy concerns can never support an unfairness claim." Instead, they simply argued that: "This standard for substantial injury overstates the appropriate level of government-enforced privacy protection on the Internet, and provides no rationale for when unsolicited commercial e-mail is unfair and when it is not. We are troubled by the possibility of an expansive and unwarranted use of the Unfairness Doctrine."[86]

Howard Beales, former Director of the FTC's Bureau of Competition, argues that "Subjective value, as opposed to emotional distress, can be a form of real injury. For example, falsely claiming that a product is kosher would cause real harm to anyone on a kosher diet."[87] More importantly, he argues that reputational harm can be "substantial injury" under the Unfairness Doctrine. In a 2003 case brought by the Bureau of Competition under Beales, the FTC successfully settled a spoofing case:

> "Spoofing" is the practice of making it appear that bulk, unsolicited commercial e-mail ("spam") comes from a third party to the transaction by placing that person or entity's e-mail address in the "from" line of the spam. As a result... spoofing portrays these innocent bystanders as duplicitous spammers, often resulting in their receiving hundreds of angry e-mails from those who had been spammed.
>
> The Commission alleged that this practice was unfair in a federal district court complaint against Brian Westby, who used spam to direct traffic to an adult website. The spam also contained deception in the subject line, tricking consumers, including children, into opening the e-mail and being subjected, in some cases, to graphic adult images. The Commission alleged that this was deceptive. The deception theory, however, does not provide any relief to those consumers who were "spoofed," because they have not relied in any way upon Westby's deception. Unfairness, however, easily reaches the problem. The harm to those consumers - both economic injury caused by damage to their computing

---

[85] Complaint, FTC v. ReverseAuction.com, Inc. File No. 0023046, (Jan. 6, 2000), available at http://www.ftc.gov/os/2000/01/reversecmp.htm.

[86] Statement of Commissioners Orson Swindle & Thomas B. Leary, FTC v. ReverseAuction.com, Inc., File No. 0023046, (Jan. 6, 2000), *available at* http://www.ftc.gov/os/2000/01/reversesl.htm.

[87] Beales Paper, *supra* note 70 (citing Timothy J. Muris, *Cost of Completion or Diminution in Market Value: The Relevance of Subjective Value*, 12 J. Legal Stud. 379 (1983)).

> systems by the huge, unexpected influx of mail, the time spent deleting thousands of e-mails, and *the injury to reputation of having their name associated with deceptive adult spam - is substantial*. Hiding the real spammer's identity has no benefit to consumers or competition, so the amount of injury, though substantial, need not be high. Finally, there is no way consumers can anticipate and protect themselves from such an invasion. Anyone with an e-mail account is vulnerable.[88]

In the *Frostwire* case, the FTC alleged a number of non-monetary harms:

> Public exposure of the types of user-originated files that FrostWire for Android shared following a default installation and set-up could increase consumers' vulnerability to identity theft; *reduce their ability to control the dissemination of personal or proprietary information* (e.g., voice recordings or intimate photographs); and increase their risk of legal liability based on prohibitions against, or limitations on, making any such files publicly available for download.[89]

In short, the FTC has staked out a bolder position on the scope of harm covered by unfairness than many realize. This is not, to be sure, the end of the debate. Since these cases have not been litigated, but rather settled before full litigation, it is not certain that this position would survive completely in court. And, on the other hand, FTC Commissioner Julie Brill has raised some difficult questions about the need to recognize harms that are probably more amorphous than ought properly to be recognized under the Unfairness Doctrine.[90]

But as noted at the outset, harms not covered by the Unfairness Doctrine should be addressed by Congress, if at all, under the basic analysis of the Unfairness Doctrine: weigh consumer harm against consumer benefit and intervene only where consumers themselves cannot reasonably avoid the harm, such as through more effective privacy controls. Congress might eventually choose to deem certain practices injurious so that the FTC will need to apply only the other elements of the test. The Unfairness Doctrine contemplates such action through its second prong, clearly established public policy.

The FTC can, however, help to clarify this uncertainty by convening a public workshop on its unfairness authority, with a special emphasis on what it considers the proper definition of harm. Ideally, such a workshop would produce guidelines building on the 1980 Unfairness Policy Statement adequate to help companies predict how to build new and innovative services without running afoul of the unfairness authority. If the FTC pushes the boundaries of harm

---

[88] Beales Paper, *supra* note 70*; See also* FTC v. Westby, No. 03-C-2540 (N.D. Ill. 2003), http://www.ftc.gov/os/2003/09/marriedcomp.pdf.

[89] F.T.C. v. Frostwire L.L.C., No. 11-23643-CV-GRAHAM (S.D. Fla. 2011), at 17. The last claim appears to refer to, *inter alia*, legal restrictions on, for example, making photographs of others publicly available without their consent.

[90] FTC Commissioner Julie Brill, *Big Data, Big Issues*, Remarks at Fordham University School of Law (Mar. 2, 2012), http://www.ftc.gov/speeches/brill/120228fordhamlawschool.pdf.

too far, Congress should intervene, as it did when it ordered the FTC to prepare its policy statements on unfairness and deception in the early 1980s.

F. The Use of Unfairness Authority to Supplement Self-Regulation

While self-regulation does not constitute established public policy adequate to justify an unfairness action on its own (if violated by a company that never acceded to a voluntary code of conduct, therefore making a deception action impossible), self-regulation may *indirectly* bolster an unfairness action—as the *Frostwire* case implies. This nuanced distinction is important to fulfilling the White House Report's promise that "There is no Federal regulation at the end of the process, and codes will not bind any companies unless they choose to adopt them."[91]

Prior to 1983, the Commission considered industry practice as well as statutes and the common law in determining whether a practice violated public policy. But the 1983 Unfairness Policy Statement implies that industry practice may play only a limited role in determining whether a practice violates public policy.[92] The 1994 amendment to the FTC Act goes a step further and declares that "public policy considerations may not serve as a primary basis for [an unfairness] determination."[93] Thus, the precise significance of industry practice remains somewhat unclear—a question that merits clarification by the FTC.

This means that industry practice, such as might be established through self-regulation, will primarily influence the consumer injury prong of unfairness, which the FTC has called "the primary focus of the FTC Act," and which can, "by itself it can be sufficient to warrant a finding of unfairness."[94]

Specifically, in the *Frostwire* case settled late last year, the FTC's unfairness argument relied, in significant part, on the fact that it was not standard industry practice to "allow the public disclosure of private files by default"[95] in establishing two of the three prongs required by the FTC's 1980 Unfairness Policy Statement. Under the third prong, the FTC argued that "a significant number of consumers using Frostwire for Android could not reasonably avoid the unwitting public sharing of their private files. These consumers would not have understood that FrostWire for Android operated in the manner described above from either the Defendants' disclosures or from prior experience with other software."[96] Under the second prong, the FTC argued that "the design and default settings [of Frostwire for Android] provided

---

[91] *Id*. at 24.

[92] 1983 FTC Unfairness Policy Statement ("To the extent that the Commission relies heavily on public policy to support a finding of unfairness, the policy should be clear and well-established. In other words, the policy should be declared or embodied in formal sources such as statutes, judicial decisions, or the Constitution as interpreted by the courts, rather than being ascertained from the general sense of the national values.").

[93] 15 U.S.C. § 45(n)

[94] 1983 FTC Unfairness Policy Statement.

[95] *Frostwire Complaint* at 17.

[96] *Id.* at 16.

few or no countervailing benefits to consumers or competition. Configuring software applications to allow the public disclosure of private files by default runs counter to standard software development guidance, and counter to established practices in the development of file-sharing applications."[97]

It would, of course, have been better—from the perspective of crafting predictable legal standards—if a court had weighed such arguments in an adversarial proceeding and provided guidance on where, exactly, to draw the line on both counts. But both arguments would likely have prevailed in court, had the FTC not settled the case. In this sense, such settled complaints form the basis of a quasi-common law of unfairness (or deception) that is at least adequate to allow companies wrestling with technological change to predict with reasonable confidence what the FTC is likely to consider a violation of Section V of the FTC Act.

The FTC's first argument hinges on their claim that "Nothing in the FrostWire for Android installation and set-up process, or the application's user interface, adequately informed consumers that the application operated in this manner."[98] In this context, the inconsistency of a practice (in this case, public disclosure of private files by default from a peer-to-peer mobile application) with standard industry practice speaks to whether it would have occurred to the reasonable consumer to investigate (a) which files the software made publicly available and (b) how to change the default setting. Simply put, the failure of transparency makes industry standards more dispositive of whether consumers would rightly expect a harmful practice.

The FTC's second argument—that industry standard for software design bear on the analysis of countervailing benefits to consumers or competition—seems somewhat more tenuous but still convincing in this case. While the FTC did not elaborate on this point (as it would have had to do before a judge had the case not been settled), it seems reasonable to argue that compliance with industry standards can benefit consumers both by lowering product design costs and also by lowering the non-monetary costs to users of learning and using a particular product interface. This is not to say that non-compliance with such standards is itself a harm, but it certainly is not a benefit if the non-compliant user interface shares sensitive information by default and makes it extremely difficult for consumers to realize this and change the necessary setting. Of course, more important than this lack of benefit is that the default sharing setting in this case did not seem to provide users a "countervailing" benefit sufficient to outweigh the potential harm flowing from the inadvertent disclosure of all the files on a user's Android device.

In summary, the *Frostwire* case does *not* stand for the proposition that industry self-regulation necessarily binds non-participating companies in its prohibitions on specific practices, but rather for the proposition that, if a company engages in a practice that diverges from industry practice *and* meets the other required elements of unfairness (causing a "substantial injury" that is "not be outweighed by any countervailing benefits to consumers or competition"), its

---

[97] *Id.*at 17.

[98] *Id.*at 16.

burden of empowering consumers to avoid that practice grows as the degree of divergence of industry practice increases.[99] Thus, the Unfairness Doctrine already offers the FTC a tool for implementing the second prong of the new framework it proposes in the FTC [Draft] Report: "For data practices that are not 'commonly accepted,' consumers should be able to make informed and meaningful choices."[100]

Concretely, then, *Frostwire* means that at least some companies that choose not to accede to the standards established by the self-regulatory process envisioned by the White House Report may have to engage in a heightened degree of "Privacy by Design" planning to analyze their non-compliant privacy practices under an unfairness analysis. Depending on their analysis of consumer harms and benefits, they may feel obliged to build accordingly more robust, and more usable, user interfaces that inform the consumer as to privacy defaults and how to change them.

This is precisely as it should be: Using its unfairness authority, the FTC can thus build on self-regulation *without* forcing compliance with self-regulation—in which case self-regulation, no matter how "voluntary" at its outset, would become co-regulation: just another vehicle for imposing top-down solutions on a complex ecosystem that requires, as the Report notes, the "flexibility, speed, and decentralization" that only true self-regulation can provide.

Yet the self-regulatory process is no less voluntary because companies that do not sign on to self-regulatory codes of conduct may be subject to somewhat elevated risks of unfairness enforcement actions for practices that diverge from industry practices established through self-regulation. But it *is* important that industry understand that the FTC's unfairness authority may play an increasingly important role as the U.S. privacy regime evolves towards more robust self-regulation. In this sense, it is that much more unfortunate that neither the White House Report nor the FTC Report does more to explain this seemingly esoteric and under-used, but extremely important, area of law. The FTC workshop and guidelines on unfairness proposed above should specifically consider how unfairness might apply to non-compliance with self-regulatory codes of conduct.

G. Self-Regulatory Policing

Robust self-regulation should involve industry enforcing the requirements on its own—in addition to FTC enforcement. The Digital Advertising Alliance has coordinated with the Better Business Bureau on just such a self-regulatory enforcement program.[101] If successful in demonstrating compliance and/or bringing enforcement actions against non-compliant companies, this enforcement program could be a model for other self-regulatory enforcement programs.

---

[99] This responsibility would, of course, also grow in proportion to the substantiality of the injury that could result from that practice, and in inverse proportion to the benefits from the practice.

[100] 2010 FTC Report at vi; *see also id*. at 40.

[101] Jack Marshall, DAA Steps Up Enforcement of Self-Regulatory Program, May 23, 2011, http://www.clickz.com/clickz/news/2073203/daa-steps-enforcement-self-regulatory-program

H. Private Ordering through Contract

Just as the White House Report acknowledges the importance of self-regulation, it also recognizes the critical importance of private ordering through contract to ensuring effective enforcement of privacy rules. Under the principle of Individual Control:

> When consumer-facing companies contract with third parties that gather personal data directly from consumers (as is the case with much online advertising), they should be diligent in inquiring about how those third parties use personal data and whether they provide consumers with appropriate choices about collection, use,and disclosure.[102]

And under the Accountability principle:

> Companies that disclose personal data to third parties should at a minimum ensure that the recipients are under enforceable contractual obligations to adhere to these principles, unless they are required by law to do otherwise. … if a company transfers personal data to a third party, it remains accountable and thus should hold the recipient accountable—through contracts or other legally enforceable instruments—for using and disclosing the data in ways that are consistent with the Consumer Privacy Bill of Rights.[103]

Structured disclosures could help to promote compliance with such principles by making it more immediately evident (and potentially searchable) whether a company's partners abide by at least the same privacy protections. Or, structured disclosures could be used to identify who a company's partners are and directly link to their privacy policies.

IX. Privacy Regulation as International Trade Barrier

A final word about enforcement: selective enforcement may be a tool for invidious discrimination by national privacy regulators, most notably by European Data Protection Authorities against American companies. Yet neither the White House Report nor the FTC Report discuss the ways discriminatory enforcement of privacy laws against American companies burden international trade in data and the products and services enabled by data—or how to ensure that our own regulations do not do the same to foreign companies. In fact, the Administration has already recognized that privacy protections, however well-intentioned can, in fact, function as barriers to international trade. At last September's APEC meeting, U.S. Ambassador Phillip Verveer warned that privacy regulations that could slow adoption of cloud services:

> In these circumstances, we would expect every economy to welcome cloud services without regard to the national origin of their producers. But there are

[102] White House Report at 11

[103] *Id.* at 21.

> complications. One of the big ones is the limitations on trans-border data flows …. It is very important, however, that we not unnecessarily sacrifice the economic advantages inherent in cloud computing in our arrangements to protect personal privacy. Stated more directly, we should not let our quest for effective privacy mechanisms become a barrier to international trade in cloud services.[104]

This concept requires further conceptual development but it certainly deserves more attention.[105] It could also be the subject of a very productive workshop, perhaps convened by the Commerce Department.

[104] Patrick Ryan, *Cloud Services and International Trade*, Google Enterprise Blog, (Oct. 13, 2011), http://googleenterprise.blogspot.com/2011/10/cloud-services-and-international-trade.html.

[105] *See generally*, Bob Boorstin, *Promoting Free Trade for the Internet Economy*, Google Pub. Pol'y Blog (Nov. 15, 2010), http://googlepublicpolicy.blogspot.com/2010/11/promoting-free-trade-for-internet.html.