Comments of
Berin Szoka, President
TechFreedom[1]

to the

National Telecommunications and Information Administration

on the

Multistakeholder Process to Develop Consumer Data Privacy Codes of Conduct[2]

Avoiding "failure by design" in the multistakeholder process envisioned by NTIA will depend on answers to the following questions:

1. What role will government play?
2. Just how "open" and "transparent" must the process be?
3. How may civil society groups participate in the process?
4. By whom will self-regulatory codes of conduct be subject to approval?
5. Regardless of who votes, what will be the mechanism for voting?
6. Will there be a shot clock for the process?
7. How will the initial selection of issues work?
8. How exactly will self-regulatory codes of conduct be updated?

In particular, if industry is to reach consensus on improving privacy practices, they must be able to negotiate in private. Moreover, if self-regulation is to deliver the "flexibility, speed, and decentralization" necessary to forge workable privacy protections that also promote innovation, as the White House hopes, it must be up to industry to vote on codes of conduct. Privacy advocates can certainly inform and shape the outcome of the self-regulatory process even without voting on its outcome.

---

[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. These comments are adapted from testimony he gave before the House Energy & Commerce Committee's Subcommittee on Commerce, Manufacturing, and Trade hearing, entitled, "Balancing Privacy and Innovation: Does the President's Proposal Tip the Scale?," on March 29, 2012 (*Szoka Testimony*). *See* http://tch.fm/GY7Xyk

[2] http://www.ntia.doc.gov/federal-register-notice/2012/multistakeholder-process-develop-consumer-data-privacy-codes-conduct

I. Introduction

The central challenge facing policymakers on privacy is three-fold:

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

Unfortunately, the privacy debate has until now focused mostly on the first part, crafting the right principles. In my Congressional testimony last week, I reminded the House Energy & Commerce Committee's Subcommittee on Commerce, Manufacturing, and Trade that the actual Bill of Rights requires privacy protection *from* government—and that privacy protection *by* government must be approached by balancing the risks associated data with its benefits. The law should punish clear abuses while empowering consumers to choose for themselves to the greatest degree possible, as consumer protection law has always done. Effective enforcement is essential to any system of privacy protection, suggesting that Congress's first job should be to ensure the FTC has the resources it needs to use its existing enforcement authority not only aggressively, but also wisely, in full recognition of these trade-offs.

But I gave credit to both President Obama's proposed "Consumer Data Privacy Framework"[3] and the FTC's Report[4] for wisely recognizing not only the central importance of the second issue (transposition from abstract principles to concrete rules), but also that the "flexibility, speed, and decentralization necessary to address Internet policy challenges"[5] can come only from a self-regulatory process such as the Commerce Department has proposed to facilitate.[6]

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."[7] 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."[8] (This essentially affirms what the FTC said in its 1999 report on privacy: "[S]elf-

---

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

[7] *Id*. at 23.

[8] *Id*. at 24.

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."[9])

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."[10] 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.

II. The Role of Government

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."[11] 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. Indeed, the principles in the White House Report all require great subtlety in their application if they are to serve consumers well, as I explained in my testimony.[12]

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.

While the experience of the Digital Advertising Alliance,[13] 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.[14] However admirable the end result, the more

---

[9] 1999 FTC Report, Self-Regulation and Privacy Online, at 6, http://www.ftc.gov/opa/1999/07/report1999.shtm .

[10] White House Report at 24.

[11] *Id*. at 24.

[12] *Szoka Testimony* at 7 (discussing the individual control principle).

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

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

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.

III. Transparency

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. A process that balances the need for transparency with the need for candid negotiation might look something like the following:

1. Selection of issues to be addressed (public)
2. Initial meeting on each focused topic to set agenda (public)
3. Industry negotiations (private: industry-only)
4. Discussions of industry draft (private: industry and civil society participants under NDA)
5. Industry revisions (private: industry-only)
6. Discussions of industry revised draft (public)
7. Industry revisions (private: industry-only)
8. Voting (public: total vote percentage; private: specific company votes)
9. *Publication of final code of conduct*
10. *Implementation*

Both in testimony by Secretary Lawrence Strickling at last week's hearing,[15] and in public comments made today by Deputy Chief Technology Officer Daniel Weitzner,[16] the Administration has attempted to steer a middle ground, suggesting that, while the official process must be entirely public, "we're not going to try to prevent anyone from having conversations that are quiet," to quote Weitzner. While this could allow the Administration to claim maximum transparency while still allowing steps 3-5 and 7 above to take place in private (as indeed they must), it raises three problems.

---

[15] http://energycommerce.house.gov/hearings/hearingdetail.aspx?NewsID=9404

[16] Tony Romm, Transparency an issue in privacy talks, Politico, April 2, 2012 ("'I'd also say that the process of coming to consensus is always complicated, and we're not going to try to prevent anyone from having conversations that are quiet.' More important, he said, is that 'what comes out of the process, the agreements that come out, have received the broadest possible public input.'").

First, splitting the proceedings in this fashion may simply prove unworkable, discouraging participation and slowing the process.

Second, even if it could be done, designing the official process such that the hard work of negotiation must take outside it, in private, may undermine the legitimacy of the process, rather than help it. While a broad range of stakeholders have expressed support for the process of self-regulation now, the self-regulatory process will be denounced by those who have long pushed for prescriptive government regulation, no matter what the outcome of that process. It seems equally like that, despite the Administration's efforts to assuage European concerns about the adequacy of our privacy protections, many in Europe will not accept the legitimacy of our self-regulatory process—if only because it does not go as far as they would like in restricting the free flow of data that has made America the leader of the global digital economy. It would be better for the Administration to defend, from the start, the legitimacy of the hybrid public/private process that even it acknowledges will be necessary for self-regulatory standard-setting to succeed.

Finally, it is particularly important that voting take place in private. Without a secret ballot, companies may simply decline to participate in the first place. Without an officially sanctioned, private voting process, the final decision about approval will simply take place in backroom deals cut between the largest players, potentially at the exclusion of smaller players. In this sense, setting an impossible standard (voting in public) could deny us the next-best thing: voting that is not visible to the public, but *is* visible to other industry participants.

IV. Civil Society Participation

How may 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.[17] 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.

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

V. Voting Eligibility

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"[18] 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."[19]

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 advocacy groups cannot attempt to use such grassroots pressure to influence the self-regulatory process.

VI. Voting Mechanisms

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.[20] Commissioner Rosch's concern about the danger of capture by industry leaders is worth noting.[21] 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

---

[18] White House Report at 24.

[19] 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.

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

[21] "[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.

increase its representation in the United Nations by insisting that Soviet Republics like Byelorussia and Ukraine deserved their own seats.[22]

VII. Timing

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.

VIII. Issue Selection

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."[23] 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[24]), 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"[25]). Other topics that may merit attention include the portability of user data, interoperability of privacy controls, and machine-readable disclosures (discussed above).

IX. Ensuring Self-Regulation Remains Dynamic

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

---

[22] *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.

[23] White House Report at 26.

[24] 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.

[25] FTC Staff Report at 68-70.

changes."[26] 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."[27] 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 open source standards)? If "Congress could prescribe a renewal period for codes of conduct," what would be required to renew and extend them?

[26] White House Report at 27.

[27] *Id.*