

June 2014

The Promise and Shortcomings of Privacy Multistakeholder Policymaking: A Case Study

Omer Tene

J. Trevor Hughes

Follow this and additional works at: <https://digitalcommons.minelaw.maine.edu/mlr>



Part of the [Privacy Law Commons](#)

Recommended Citation

Omer Tene & J. T. Hughes, *The Promise and Shortcomings of Privacy Multistakeholder Policymaking: A Case Study*, 66 Me. L. Rev. 437 (2014).

Available at: <https://digitalcommons.minelaw.maine.edu/mlr/vol66/iss2/5>

This Article is brought to you for free and open access by the Journals at University of Maine School of Law Digital Commons. It has been accepted for inclusion in Maine Law Review by an authorized editor of University of Maine School of Law Digital Commons. For more information, please contact mdecrow@maine.edu.

THE PROMISE AND SHORTCOMINGS OF PRIVACY MULTISTAKEHOLDER POLICYMAKING: A CASE STUDY

Omer Tene and J. Trevor Hughes

- I. INTRODUCTION
- II. FORMAL POLICYMAKING
- III. MULTISTAKEHOLDER POLICYMAKING: A PROMISING PATH?
 - A. *FTC Support*
 - B. *Department of Commerce Support*
 - C. *European Union Support*
- IV. ASSESSING MULTISTAKEHOLDER PROCESSES IN PRACTICE: DO NOT TRACK
 - A. *Expeditious Decision-Making*
 - 1. *Decision-Making Rules*
 - 2. *Representation and Composition*
 - 3. *Delay Tactics*
 - 4. *The Role of the Chair*
 - 5. *Drafting a Straw Man*
 - 6. *Web-Based Communications Tools*
 - B. *Informed by Industry Knowledge and Expertise*
 - 1. *Arguing over Facts*
 - 2. *Engineers vs. Lawyers*
 - C. *Fostering Collaboration and Compliance*
 - 1. *Good Spec; No Implementation*
 - 2. *Incentive to Comply?*
 - 3. *External Disruptions*
- V. CONCLUSION

THE PROMISE AND SHORTCOMINGS OF PRIVACY MULTISTAKEHOLDER POLICYMAKING: A CASE STUDY

*Omer Tene and J. Trevor Hughes**

A: I think the notion of a multistakeholder process was bolstered, not by thinking that it will work necessarily, but rather because it's so easy to call for. That's a classic line: "we need a dialogue!" You don't have to take a position on the issue; you don't have to do anything about an issue to say, "We should talk about it."

Q: So, it's basically a cop out?

A: I think that's right.¹

I. INTRODUCTION

With formal privacy policymaking processes mired in discord, governments and regulators in the United States and Europe have turned to the private sector seeking assistance and solutions. Multistakeholder-driven self-regulation and co-regulation have been pursued in a variety of contexts ranging from online privacy and transparency for mobile applications to protection of transborder data flows. This Article focuses on one such process, the World Wide Web Consortium (W3C) discussion of a Do Not Track (DNT) standard, as a case study.² It critically analyzes the procedural pitfalls, which hampered the quest to reach a compromise solution acceptable by groups with diametrically opposed interests, including industry players, government regulators, and privacy advocates. It is based on a series of interviews that the Authors conducted with participants in the process, including leading industry, civil society, and government players.³

Proponents of multistakeholder processes, including the U.S. government, suggest that this mode of policymaking benefits from important advantages, including an opportunity to coopt industry experts, move swiftly to conclusion, and garner industry support.⁴ The reality, however, is that the W3C process featured

* Omer Tene is Vice President of Research and Education and J. Trevor Hughes President and CEO of the International Association of Privacy Professionals. The Authors would like to thank Jonathan Mayer, Joanne McNabb, John Verdi, and Alexander Hanff, as well as two additional interviewees who asked to remain anonymous, for their valuable time and thoughtful insights, and Jedidiah Bracy, Andrew Clearwater, and Sam Pfeifle for invaluable comments. Special thanks to Kelsey Finch for excellent, thorough research assistance.

1. Telephone Interview with Jonathan Mayer, Stanford University graduate student in computer science and law, and an invited expert to the W3C process (Dec. 6, 2013) [hereinafter Mayer Interview].

2. See Nick Doty & Deirdre K. Mulligan, *Internet Multistakeholder Processes and Techno—Policy Standards Initial Reflections on Privacy at the World Wide Web Consortium*, 11 J. TELECOMM. & HIGH TECH. L. 135 (2013).

3. Given that the interviews focused not on substantive issues but rather on the mechanics of the process, we allowed some of the interviewees to remain anonymous. We believe that an "off the record" discussion better captured their candid criticism and allowed them to speak freely.

4. *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy*, THE WHITE HOUSE 23-27 (Feb. 23, 2012),

few of these benefits. It was protracted, rife with hardball rhetoric and combat tactics, based on inconsistent factual claims, and under constant threat of becoming practically irrelevant due to lack of industry buy-in.

Perhaps this should not be surprising. The way DNT has been framed—as a veritable “on/off” switch for an entire *industry*—inevitably raised the stakes for a common accord.⁵ Indeed, DNT crystallizes a deep ideological divide about right and wrong in online behavior, with one side arguing that merely *collecting* users’ information is wrong, and the other side claiming a right—in fact a business imperative—to use such information for multiple goals.⁶ Add to that a healthy portion of competitive maneuvering within the industry, and you get a combusive mix.

As the discussions progressed, they became increasingly contentious and polarized, with the most extreme voices on either side of the ideological divide leading the way.⁷ Moreover, they were subject to the disruptive force of exogenous factors, not the least of which was the unilateral decision by Microsoft, a major browser maker, to automatically set DNT on by default.⁸ This development, in and of itself, may very well have been the death knell of an already a stagnant process.

Critics could argue that self-regulation would be better served without a preceding multistakeholder process. Let the industry devise rules for itself, at most soliciting comments from civil society and regulators. Yet codes of conduct drafted *by industry for industry* are often derided as a self-serving ruse intended to avert formal regulation.⁹ As one privacy advocacy organization notes, “We now have repetitive, specific, tangible examples of failed self-regulation in the area of privacy.”¹⁰

Others could argue that the W3C was ill-suited in the first place to engage in a highly divisive policy debate of this nature. Primarily a technical standard-setting body, W3C, which is run by engineers, was not prepared to resolve policy conflicts

<http://www.whitehouse.gov/sites/default/files/privacy-final.pdf> [hereinafter *White House Privacy Framework*].

5. Omer Tene & Jules Polonetsky, *To Track or “Do Not Track”: Advancing Transparency and Individual Control in Online Behavioral Advertising*, 13 MINN. J.L. SCI. & TECH. 281, 334 (2012).

6. *Id.*

7. See Laura Stampler, *Firefox Launches ‘Nuclear First Strike Against Ad Industry,’* BUS. INSIDER (Feb. 25, 2013, 9:36 AM), <http://www.businessinsider.com/firefox-to-block-third-party-cookies-2013-2#ixzz2vWG3wFFc>.

8. Brendon Lynch, *Advancing Consumer Trust and Privacy: Internet Explorer in Windows 8*, MICROSOFT ON THE ISSUES (May 31, 2012, 5:00 PM), http://blogs.technet.com/b/microsoft_on_the_issues/archive/2012/05/31/advancing-consumer-trust-and-privacy-internet-explorer-in-windows-8.aspx.

9. Chris Jay Hoofnagle, *Privacy Self-Regulation: A Decade of Disappointment*, ELEC. PRIVACY INFO. CTR. 1 (Mar. 4, 2005), <http://epic.org/reports/decadedisappoint.pdf>; Robert Gellman & Pam Dixon, *Many Failures: A Brief History of Privacy Self-Regulation in the United States*, WORLD PRIVACY FORUM 4 (Oct. 14, 2011), <http://www.worldprivacyforum.org/wp-content/uploads/2011/10/WPFselfregulationhistory.pdf>.

10. World Privacy Forum, *Comments of the World Privacy Forum Regarding the Federal Trade Commission Preliminary Staff Report, Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Business and Policymakers*, FED. TRADE COMM’N 3 (Feb. 18, 2011), http://www.ftc.gov/sites/default/files/documents/public_comments/preliminary-ftc-staff-report-protecting-consumer-privacy-era-rapid-change-proposed-framework/00376-58005.pdf.

among scores of lawyers and government affairs professionals. Its decision-making processes were fickle and revolved around a seemingly endless list of repetitive, overlapping issues.¹¹ Like Goethe's *Sorcerer's Apprentice*,¹² the W3C experienced every effort to close an issue while simultaneously opening several new ones. It is perhaps telling that after more than two years of discussions, the group has not yet been able to define the term "tracking," the *raison d'être* for the process.¹³ Rules on representation were vague and included a pay-to-play entry barrier that may have skewed the composition of the group towards more resourceful stakeholders.¹⁴

Part II of this Article analyzes the difficulties facing formal policymaking processes in the field of privacy. Rapidly evolving technologies, shifting business models, and polarized social and cultural norms complicate the quest for a simplified privacy policy. This has led policymakers to turn to the private sector for help. Part III sets forth the opportunities and risks of multistakeholder-driven self-regulatory and co-regulatory models. Part IV of the Article assesses multistakeholder processes in practice, focusing on the W3C discussion of DNT as a case study. It shows that, counter to conventional wisdom, a multistakeholder process could turn out to be neither faster moving nor more collaborative than top-down regulation, and may be set for little or no industry adoption even in the unlikely case that it is resolved. The Article does not set out to, nor does it, prove that all multistakeholder processes are destined to fail. Rather, it seeks to draw lessons from one particular attempt at multistakeholder policymaking in order to help improve new processes down the road. Part V concludes, setting forth basic recommendations for the future.

II. FORMAL POLICYMAKING

Policymaking in the field of information privacy has been laden with discord. For many years, the United States has been debating the merits, format, and sometimes contents of comprehensive privacy legislation,¹⁵ yet, there is no end to the debate in sight.¹⁶ In the European Union, where privacy law is clearly in need of reform,¹⁷ policymakers are embroiled in what seem to be endless heated discussions around the minutia of a 119-page legislative document submitted more

11. See discussion *infra* Part IV.A.3.

12. JOHANN WOLFGANG VON GOETHE, *THE SORCERER'S APPRENTICE* (Edwin Zeydel trans., 1955) (1779), available at http://germanstories.vcu.edu/goethe/zauber_e3.html.

13. See *Issue-5: What is the Definition of Tracking?*, WORLD WIDE WEB CONSORTIUM, <http://www.w3.org/2011/tracking-protection/track/issues/5> (last visited Mar. 22, 2014) (settling on a definition of "tracking" that is dependent on several additional yet-to-be resolved issues, such as an explanation of permitted tracking).

14. See discussion *infra* Part IV.A.2.

15. Joel R. Reidenberg, *Privacy Wrongs in Search of Remedies*, 54 HASTINGS L.J. 877, 897-98 (2003).

16. Somini Sengupta, *No U.S. Action, So States Move on Privacy Law*, N.Y. TIMES, Oct. 31, 2013, at A1, available at <http://www.nytimes.com/2013/10/31/technology/no-us-action-so-states-move-on-privacy-law.html>.

17. See Omer Tene, *Privacy Law's Midlife Crisis: A Critical Assessment of the Second Wave of Global Privacy Laws*, 74 OHIO ST. L.J. 1217, 1232-34 (2013).

than two years ago by the European Commission.¹⁸ The embattled legislative process periodically flares into mutual recriminations between European institutions and sometimes even national strife.¹⁹

Perhaps this should come as no surprise, given that even the basic tenets of privacy law are rife with ambiguity. For more than a century, scholars and jurists have vigorously argued over the definition of privacy,²⁰ and notwithstanding several compelling theories, the discussion continues unabated today. The framing of other foundational terms remains similarly elusive. Even where plaintiffs prove the elements of a privacy cause of action, they often run into difficulty when asked to show harm,²¹ given the lack of legal consensus over whether privacy harms are legally cognizable.²² Personally identifiable information, the most basic building block of an information privacy framework, remains one of the most contentious concepts in privacy, igniting frequent disputes between engineers and lawyers involving science, philosophy, and a healthy dosage of political spin.²³ Another charged concept is that of consent, a veritable trump card in privacy interactions, abused almost as often as it is used, and meaning dramatically different things to different people, companies, and regulators.²⁴

Privacy is highly culturally dependent, stoking persistent discord between Europe and the U.S.²⁵ Despite some convergence around high-level principles known as the Fair Information Practice Principles (FIPPs),²⁶ there continues to be significant disharmony with respect to the general place of information privacy in

18. Christopher Kuner, Cédric Burton, & Anna Pateraki, *The Proposed EU Data Protection Regulation Two Years Later*, BNA PRIVACY & SEC. L. REP. 1-2 (Jan. 2014), <http://www.wsgl.com/eudataregulation/pdf/kuner-010614.pdf>.

19. See, e.g., Kelly Fiveash, *EU Legal Eagle Legal: Data Protection Reforms 'Very Bad Outcome' for Citizens*, THE REGISTER, Dec. 9, 2013, http://www.theregister.co.uk/2013/12/09/eu_data_protection_reforms_hits_legal_roadblock; *EU To Push Ahead On Data Protection Despite UK Opposition*, EURACTIV.COM, Oct. 28, 2013, <http://www.euractiv.com/specialreport-digital-single-mar/commission-push-ahead-data-prote-news-531357>.

20. See, e.g., ALAN F. WESTIN, *PRIVACY AND FREEDOM* 7 (1967); Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477 (2006); HELEN NISSENBAUM, *PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE* 2 (2010); Julie E. Cohen, *What Privacy is For*, 126 HARV. L. REV. 1904 (2013).

21. M. Ryan Calo, *The Boundaries of Privacy Harm*, 86 IND. L.J. 1131, 1132 (2011).

22. *Id.*

23. See Paul M. Schwartz & Daniel J. Solove, *The PII Problem: Privacy and a New Concept of Personally Identifiable Information*, 86 N.Y.U. L. REV. 1814, 1816 (2011); Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701, 1704 (2010).

24. Omer Tene & Christopher Wolf, *The Draft EU General Data Protection Regulation: Costs and Paradoxes of Explicit Consent* (Future of Privacy Forum White Paper, Jan. 2013), available at <http://www.scribd.com/doc/121642539/The-Draft-EU-General-Data-Protection-Regulation-Costs-and-Paradoxes-of-Explicit-Consent>.

25. Omer Tene, *Privacy in Europe and the United States: I Know It When I See It*, CTR. FOR DEMOCRACY & TECH. BLOG (June 27, 2011), <https://cdt.org/blogs/privacy-europe-and-united-states-i-know-it-when-i-see-it>.

26. Org. for Econ. Co-Operation & Dev., *The Evolving Privacy Landscape: 30 Years After the OECD Privacy Guidelines*, in THE OECD PRIVACY FRAMEWORK 70-71 (July 11, 2013), http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf.

law.²⁷ At the risk of oversimplification, Europeans view information privacy as a fundamental human right, whereas the U.S. treats it as a matter of tort law and consumer protection.²⁸ At the same time, the parties to the cross-Atlantic discussion often seem to be talking past each other. For example, while Europe waves the “fundamental right” flag as it depicts U.S. privacy law as “inadequate,” Europeans sometimes forget that privacy is a constitutional right in the U.S., protected by the Fourth Amendment as well as through “penumbras of privacy” in the Constitution.²⁹ And while Americans tend to portray the European framework as bureaucratic and overly prescriptive, it is often U.S. law with its layers upon layers of federal and state statutes, regulatory and individual enforcement, that is daunting to operationalize.³⁰

The heart of the matter is that privacy raises genuine dilemmas and thorny legal questions. First, it consistently collides with other constitutional rights and weighty policy interests. For example, privacy often restricts freedom of speech, the cornerstone of constitutional liberties in the U.S. and a forceful fundamental right in Europe.³¹ Similarly, it often conflicts with the interests of national security and law enforcement agencies, which seek to collect as much information as possible in their intelligence gathering and enforcement operations.³² An obstacle to the free flow of information, privacy is anathema to free market theorists like Richard Posner, who pronounced it overrated, dangerous, and “really just a euphemism for concealment, for hiding specific things about ourselves from others.”³³

Second, the formation of a coherent privacy policy is impeded by the lightning speed of innovation in the technology industry. The surge in technological developments makes privacy policymaking a moving target.³⁴ Consider the laborious process in Europe for amending the Electronic Communications Privacy Directive, colloquially known as the “Cookie Directive.”³⁵ By the time the legislation, which requires users’ opt-in consent for website cookie use,³⁶ was passed, the technological landscape shifted to supplant cookies with server-side tracking alternatives and embedded device identifiers.³⁷

27. See generally Kenneth A. Bamberger & Deirdre K. Mulligan, *Privacy in Europe: Initial Data on Governance Choices and Corporate Practices*, 81 GEO. WASH. L. REV. 1529 (2013).

28. See *id.* at 1539-47.

29. *Griswold v. Connecticut*, 381 U.S. 479, 483 (1965).

30. Schwartz & Solove, *supra* note 23, at 1872-77.

31. See, e.g., *Sorrell v. IMS Health Inc.*, 131 S. Ct. 2653, 2659 (2011); *Campbell v. MGN Ltd.*, [2004] UKHL 22 [12] (U.K.); *Von Hannover v. Germany* (No. 2), 2012 Eur. Ct. H.R. 228, ¶ 69.

32. See, e.g., Jack Goldsmith, *Cyberthreat, Government Network Operations, and the Fourth Amendment*, in CONSTITUTION 3.0: FREEDOM AND TECHNOLOGICAL CHANGE 47, 57-60 (Jeffrey Rosen & Benjamin Wittes eds., 2011).

33. Richard A. Posner, *Privacy is Overrated*, N.Y. DAILY NEWS, Apr. 28, 2013, 4:19 AM, <http://www.nydailynews.com/opinion/privacy-overrated-article-1.1328656>.

34. See generally, Omer Tene, *Privacy Law's Midlife Crisis: A Critical Assessment of the Second Wave of Global Privacy Laws*, 74 OHIO ST. L.J. 1217 (2013).

35. Council Directive 2009/136, 2009 O.J. (L 337) 11 (EC).

36. *Id.* art. 2, §§ (5)-(6).

37. Kelsey Finch, *Cookie Monsters of Silicon Valley Come to Brussels*, IAPP: THE PRIVACY ADVISOR, Nov. 25, 2013,

Third, the social norms underlying privacy policy are in constant flux. With technological innovation rapidly driving new models for business and inviting new types of socialization, policymakers often have nothing more than fleeting intuitions as to what is right or wrong.³⁸ As new technologies strain our social norms, a shared understanding of privacy etiquette becomes even more difficult to capture.³⁹ Yet for businesses that make money by leveraging newly available data sources, it is critical to operationalize these subjective notions into coherent business and policy strategies. This, in turn, exerts more pressure on policymakers to deliver results expeditiously.

III. MULTISTAKEHOLDER POLICYMAKING: A PROMISING PATH?

Against this backdrop, it is clear why governments and legislatures have coopted the public for assistance in the policymaking process. The U.S. has engaged the private sector in self-regulatory efforts for more than a decade, culminating in the Obama administration's call for a structured set of multistakeholder processes as a pillar of its privacy strategy.⁴⁰ As one commentator notes, "[The FTC and DOC] argue that self-regulation can protect privacy in a more flexible and cost-effective manner than direct regulation without impeding the rapid pace of innovation in Internet-related businesses."⁴¹

Proponents of multistakeholder self-regulatory and co-regulatory solutions suggest that these modes of policymaking benefit from distinct advantages *vis-à-vis* the legislative process.⁴² They argue that these collaborative mechanisms tap into industry knowledge and expertise, producing more practical and effective rules,⁴³ can produce solutions in a more timely fashion than formal regulatory processes,⁴⁴ and are more likely to rally industry support and adoption than top-down regulation.⁴⁵ Critics argue that privacy self-regulation reflects industry subterfuge intended to avert (or at the very least delay) regulation,⁴⁶ tends to be overly lax and

https://www.privacyassociation.org/publications/cookie_monsters_of_silicon_valley_come_to_brussels.

38. Omer Tene & Jules Polonetsky, *A Theory of Creepy: Technology, Privacy and Shifting Social Norms*, 16 YALE J.L. & TECH. (forthcoming 2014) (manuscript at 2) (available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2326830).

39. *Id.*

40. *White House Privacy Framework*, *supra* note 4.

41. Ira S. Rubinstein, *Privacy and Regulatory Innovation: Moving Beyond Voluntary Codes*, 6 ISJLP 355, 356 (2011).

42. Dennis D. Hirsch, *In Search of the Holy Grail: Achieving Global Privacy Rules Through Sector-Based Codes of Conduct*, 74 OHIO ST. L.J. 1029, 1041-42 (2013) (citing Neil Gunningham & Joseph Rees, *Industry Self-regulation: An Institutional Perspective*, 19 L. & POL'Y 363, 366 (1997)); see Rubinstein, *supra* note 41, at 357-58; Jody Freeman, *Collaborative Governance in the Administrative State*, 45 UCLA L. REV. 1, 22 (1997).

43. Hirsch, *supra* note 42, at 1041-42.

44. *White House Privacy Framework*, *supra* note 4, at 23.

45. Hirsch, *supra* note 43, at 1041-42; Dennis D. Hirsch, *Going Dutch? Collaborative Dutch Privacy Regulation and the Lessons It Holds for U.S. Privacy Law*, 2013 MICH. ST. L. REV. 83, 104.

46. Hoofnagle, *supra* note 9, at 5; Gellman & Dixon, *supra* note 9, at 25. Hirsch points out that unlike self-regulation, co-regulation is less amenable to industry capture given the involvement of government and regulators. Hirsch, *supra* note 43, at 1045-46.

serve a public relations rather than a regulatory function,⁴⁷ and has a poor track record for compliance and enforcement.⁴⁸

A. FTC Support

In July 1999, the FTC issued a report to Congress titled “Self-Regulation and Online Privacy,” in which it stated that legislation to address online privacy was inappropriate in the face of industry efforts to self-regulate.⁴⁹ In evaluating the state of online privacy self-regulation, the report stressed that “self-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.”⁵⁰ The FTC report and preceding consultations spawned a number of self-regulatory efforts, including the Network Advertising Initiative (NAI) and the BBBOnline Privacy Program, a subsidiary of the Council of Better Business Bureaus.⁵¹

Over the years, the FTC’s support for and interest in a self-regulatory privacy framework has waxed and waned.⁵² In 2010, as privacy in online behavioral

47. COLIN J. BENNETT & CHARLES D. RAAB, *THE GOVERNANCE OF PRIVACY: POLICY INSTRUMENTS IN GLOBAL PERSPECTIVE* 154 (2006).

48. Hirsch, *supra* note 43, at 1043; Gellman & Dixon, *supra* note 9, at 4, 6, 9.

49. Press Release, Fed. Trade Comm’n, “Self-Regulation and Privacy Online,” FTC Report to Congress (July 13, 1999) (available at <http://www.ftc.gov/news-events/press-releases/1999/07/self-regulation-and-privacy-online-ftc-report-congress>); see *Self-Regulation and Privacy Online: Hearing Before the Subcomm. on Comm’n of the S. Comm. on Commerce, Sci., & Transp.*, 106th Cong. 4-5 (1999), available at http://www.ftc.gov/sites/default/files/documents/public_statements/prepared-statement-federal-trade-commission-self-regulation-and-privacy-online/privacyonlinetestimony.pdf (prepared statement of Robert Pitofsky, Chairman, Fed. Trade Comm’n).

50. Fed. Trade Comm’n, *supra* note 49.

51. See ROBERT GELLMAN & PAM DIXON, *WORLD PRIVACY FORUM, MANY FAILURES: A BRIEF HISTORY OF PRIVACY SELF-REGULATION IN THE UNITED STATES 7-8* (Oct. 14, 2011), available at <http://www.worldprivacyforum.org/wp-content/uploads/2011/10/WPFselfregulationhistory.pdf>. For information on how these programs have evolved, see *BBB EU Safe Harbor Program*, COUNCIL FOR BETTER BUS. BUREAUS, <http://www.bbb.org/council/eusafeharbor> (last visited Apr. 21, 2014); *NAI Code Enforcement*, NETWORK ADVER. INITIATIVE, <http://www.networkadvertising.org/code-enforcement> (last visited Apr. 21, 2014).

52. For example, just a year after its 1999 report advocating self-regulation and legislative restraint, the FTC reported to Congress that, although there had been improvement in industry self-regulatory efforts, the robustness of these processes was unsatisfactory. *Privacy Online: Fair Information Practices in the Electronic Marketplace, a Report to Congress*, FED. TRADE COMM’N ii (May 2000), <http://www.ftc.gov/sites/default/files/documents/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission-report/privacy2000text.pdf>. Accordingly, a majority of the commissioners concluded that it was time for legislation requiring online businesses to comply with the FIPPs. *Id.* at 36-38. In December 2007, following a “Behavioral Advertising Town Hall” that led to a public discussion about the need to address privacy concerns in this area, the FTC issued for public comment a set of proposed principles to encourage and guide industry self-regulation. Press Release, Fed. Trade Comm’n, *FTC Staff Revises Online Behavioral Advertising Principles* (Feb. 12, 2009) (available at <http://www.ftc.gov/news-events/press-releases/2009/02/ftc-staff-revises-online-behavioral-advertising-principles>). In 2009, the FTC issued a report, titled “Self-Regulatory Principles for Online Behavioral Advertising,” setting forth revisions to proposed principles to govern self-regulatory efforts in this area. *FTC Staff Report: Self-Regulatory Principles for Online Behavioral Advertising*, FED. TRADE COMM’N (Feb. 2009), <http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-staff-report-self-regulatory-principles-online-behavioral-advertising/p085400behavadreport.pdf>. Commissioner Jon Leibowitz issued a separate concurring statement

advertising remerged as a primary item on the FTC's agenda, self-regulation was once again put forth as a possible solution.⁵³ To be sure, the FTC stated in its Preliminary Staff Report that "industry efforts to address privacy through self-regulation have been too slow, and up to now have failed to provide adequate and meaningful protection."⁵⁴ Yet, it also made clear that it "supports a more uniform and comprehensive consumer choice mechanism for online behavioral advertising, sometimes referred to as 'Do Not Track,'" adding that "[s]uch a universal mechanism could be accomplished by legislation or potentially through robust, enforceable self-regulation."⁵⁵

In its final report, issued in 2012, the FTC noted that "industry has made significant progress in implementing Do Not Track," referring to tools developed by browser vendors and commitments undertaken by the Digital Advertising Alliance (DAA), a broad coalition of industry groups.⁵⁶ Yet, the FTC particularly emphasized the work done by the W3C Tracking Protection Working Group (the "Working Group"), noting that "[t]he W3C group has made substantial progress toward a standard that is workable in the desktop and mobile settings."⁵⁷ Stressing the multistakeholder nature of this effort, the FTC elaborated that "the W3C Internet standards-setting body has gathered a broad range of stakeholders to create an international, industry-wide standard for Do Not Track. The Working Group includes a wide variety of stakeholders, including DAA members; other U.S. companies; international companies; industry groups; and public-interest groups."⁵⁸ Suffice it to say that, as further discussed *infra*, the W3C process failed to deliver on its promise.

attached to the report, noting, "I write separately to ensure that the Report's endorsement of self-regulation is viewed neither as a regulatory retreat by the Agency nor an imprimatur for current business practice." *FTC Staff Report: Self-Regulatory Principles for Online Behavioral Advertising, Concurring Statement of FTC Comm'r Jon Leibowitz*, FED. TRADE COMM'N 1 (Feb. 2009), http://www.ftc.gov/sites/default/files/documents/public_statements/concurring-statement-commissioner-jon-leibowitz-ftc-staff-report-self-regulatory-principles-online/p085400behavdleibowitz.pdf. He also states, "Industry needs to do a better job of meaningful, rigorous self-regulation or it will certainly invite legislation by Congress and a more regulatory approach by our Commission. Put simply, this could be the last clear chance to show that self-regulation can – and will – effectively protect consumers' privacy in a dynamic online marketplace." *Id.* This report, too, prompted the industry to launch a number of self-regulatory initiatives, including the development of new codes of conduct and online tools to allow consumers more control over the receipt of targeted advertising. See *DAA Announces Guidance for Self-Reg Principles in Mobile Environment*, DIGITAL ADVER. ALLIANCE, <http://www.aboutads.info> (last visited Apr. 21, 2014).

53. *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers, Preliminary FTC Staff Report*, FED. TRADE COMM'N iii (Dec. 2010), <http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-bureau-consumer-protection-preliminary-ftc-staff-report-protecting-consumer/101201privacyreport.pdf> [hereinafter *FTC Staff Report*]; see also DIGITAL ADVER. ALLIANCE, *supra* note 52.

54. *FTC Staff Report*, *supra* note 53.

55. *Id.* at 66.

56. *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers*, FED. TRADE COMM'N 13 (Mar. 2012), <http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf>.

57. *Id.* at 5.

58. *Id.* at 54.

B. Department of Commerce Support

Not only the FTC, but also the U.S. Department of Commerce, has actively promoted multistakeholder policymaking. In its main policy statement on privacy to date, the Obama administration increased its reliance on the success of multistakeholder-generated enforceable codes of conduct.⁵⁹ The administration promoted: a statutory consumer privacy bill of rights,⁶⁰ which has yet to materialize and many doubt that it will,⁶¹ strengthening FTC enforcement,⁶² which similarly hinges on legislation; and improving global interoperability,⁶³ which is a lofty goal, albeit without a clear success matrix. Hence, fostering multistakeholder processes to develop enforceable codes of conduct remains the main actionable item in the administration's strategy.

The administration promised to “convene open, transparent forums in which stakeholders who share an interest in specific markets or business contexts will work toward consensus on appropriate, legally enforceable codes of conduct.”⁶⁴ It encouraged all relevant parties to engage, including “individual companies, industry groups, privacy advocates, consumer groups, crime victims, academics, international partners, State Attorneys General, [and] Federal civil and criminal law enforcement representatives.”⁶⁵ Citing the success of Internet standard setting bodies, such as the Internet Engineering Task Force (IETF) and W3C, as well as the Internet Corporation for Assigned Names and Numbers (ICANN), a nonprofit corporation that coordinates the technical management of the domain name system, the administration posited that multistakeholder processes underlie many of the institutions responsible for the Internet's success.⁶⁶ It believed that multistakeholder processes could achieve results with more flexibility, speed, and decentralization than formal regulatory processes.⁶⁷

The administration tasked the National Telecommunications and Information Administration (NTIA), a Department of Commerce agency responsible for advising the President on telecommunications and information policy issues, with convening and facilitating the discussion.⁶⁸ However, the administration did not envisage the NTIA as a decision-maker, stating that the “NTIA's role will be to help the parties reach clarity on what their positions are and whether there are options for compromise toward consensus, rather than substituting its own judgment.”⁶⁹ Recognizing that a consensus rule can reward intransigence, the administration proposed that “the parties should discuss and set out rules or procedures at the outset of the process to govern how the group will reach an

59. *White House Privacy Framework*, *supra* note 4, at 2.

60. *Id.* at 1-2, 35-36.

61. *See* Sengupta, *supra* note 16.

62. *White House Privacy Framework*, *supra* note 4, at 2, 29-30.

63. *Id.* at 2-3, 31-33.

64. *Id.* at 2.

65. *Id.* at 23.

66. *Id.* at 25.

67. *Id.* at 23-24.

68. *Id.* at 26.

69. *Id.* at 27.

orderly conclusion, even if there is not complete agreement on results.”⁷⁰ The discussions were intended to produce codes of conduct for various industry groups or sectors.⁷¹

The administration foresaw a co-regulatory model,⁷² featuring multistakeholder created codes of conduct backed by FTC enforcement.⁷³ Under Section 5 of the FTC Act, the FTC is empowered to enforce a code of conduct pursuant to a company’s voluntary decision to enroll.⁷⁴ The administration suggested that companies’ incentive to engage in the process would be twofold: building consumer trust and benefitting from a safe harbor to FTC enforcement.⁷⁵

Moreover, the administration envisaged that the FTC would have explicit statutory authority to review codes of conduct against prospective privacy legislation.⁷⁶ Importantly, “the Administration recommends . . . giving the FTC the authority to grant a ‘safe harbor’—that is, forbearance from enforcement of the statutory Consumer Privacy Bill of Rights—to companies that follow a code of conduct that the FTC has reviewed and approved.”⁷⁷ In the absence of such legislation, however, these new FTC powers are weakened, given that there is no law to assess the code of conduct against, and no law from which to grant immunity. Hence, if the administration fails to deliver on the statutory promise in its strategy, the FTC would have to revert to its current stance: enforcement only against companies that voluntarily and publicly commit to following a code of conduct and then fail to deliver.

C. European Union Support

Not only the U.S., but also the EU, promotes self- and co-regulation. Under Article 27 of the European Data Protection Directive:

- (1) The Member States and the Commission shall encourage the drawing up of codes of conduct intended to contribute to the proper implementation of the national provisions adopted by the Member States pursuant to this Directive, taking account of the specific features of the various sectors.
- (2) Member States shall make provision for trade associations and other bodies representing other categories of controllers which have drawn up draft national codes or which have the intention of amending or extending existing national

70. *Id.* at 27.

71. *Id.* at 26.

72. Dennis Hirsch defines co-regulation as a process in which government and private parties share responsibility for development and enforcement of regulatory rules; they may do so by splitting the tasks up: “For example, government might set the overall goals but then allow industry to set and enforce the standards. Or, more commonly, government and the private sector might perform one or more of the tasks together.” Dennis D. Hirsch, *The Law and Policy of Online Privacy: Regulation, Self-Regulation, or Co-Regulation?*, 34 SEATTLE U. L. REV. 439, 465 (2011).

73. *White House Privacy Framework*, *supra* note 4, at 26-27.

74. *Id.* at 27, 29.

75. *Id.* at 24.

76. *Id.* at 37.

77. *Id.*

codes to be able to submit them to the opinion of the national authority.⁷⁸

National data protection authorities and the Article 29 Working Party are authorized to review and confirm the compliance of a multistakeholder code of conduct with European or national data protection law.⁷⁹ Interestingly, this framework has come short of generating co-regulatory zeal. To date, nearly twenty years after the introduction of the European Data Protection Directive, only *one* code of conduct has been submitted for regulatory approval—by the Federation of European Direct and Interactive Marketing.⁸⁰

On January 25, 2012, the European Commission proposed a new General Data Protection Regulation that would replace the European Data Protection Directive.⁸¹ Like the European Data Protection Directive, the proposed General Data Protection Regulation would endorse the development of sector-based codes of conduct, which could then be submitted for regulatory approval.⁸² Under Article 38 of the proposed General Data Protection Regulation, such codes of conduct would be eligible for approval by the European Commission.⁸³ Furthermore, Article 39 of the proposed General Data Protection Regulation would authorize new co-regulatory mechanisms, namely “the establishment of data protection certification mechanisms and of data protection seals and marks.”⁸⁴ Such programs, developed by the private sector and ratified by the European Commission, would allow individuals to quickly assess the level of data protection provided by companies.⁸⁵

IV. ASSESSING MULTISTAKEHOLDER PROCESSES IN PRACTICE: DO NOT TRACK

Despite best intentions, recent efforts at multistakeholder policymaking leave much to be desired. This Article focuses on a test case, the W3C discussion of a DNT standard, which at this point, more than two years after its launch, appears to

78. Council Directive 95/46, art. 27(1)-(2), 1995 O.J. (L281) 31 (EC).

79. *Id.* at art. 28(3)-(4).

80. The only code submitted for approval was the Federation of European Direct and Interactive Marketing’s (FEDMA) Community Code, which provides a legal safe harbor in all European Member States to adherent direct marketing firms, and was approved by the Article 29 Data Protection Working Party in 2003. WORKING PARTY 77, OPINION 3/2003 OF THE ARTICLE 29 DATA PROTECTION WORKING PARTY ON THE EUROPEAN CODE OF CONDUCT OF FEDMA FOR THE USE OF PERSONAL DATA IN DIRECT MARKETING (June 13, 2003), available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2003/wp77_en.pdf (approving FEDMA code); see also WORKING PARTY 174, OPINION 4/2010 OF THE ARTICLE 29 DATA PROTECTION WORKING PARTY ON THE EUROPEAN CODE OF CONDUCT OF FEDMA FOR THE USE OF PERSONAL DATA IN DIRECT MARKETING (July 13, 2010), available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2010/wp174_en.pdf (approving annex to the FEDMA code covering online marketing).

81. EUR. COMM’N, PROPOSAL FOR A REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA AND ON THE FREE MOVEMENT OF SUCH DATA (GENERAL DATA PROTECTION REGULATION) COM (2012) 11 final (Jan. 25, 2012), available at http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf.

82. *Id.* at ch. IV, § 5.

83. *Id.*

84. *Id.* See ROWENA RODRIGUES ET AL., EUR. COMM’N JOINT RES. CTR. INST. FOR THE PROT. & SEC. OF THE CITIZEN, EU PRIVACY SEALS PROJECT, INVENTORY AND ANALYSIS OF PRIVACY CERTIFICATION SCHEMES, FINAL REPORT STUDY DELIVERABLE 1.4, at 12 (Dec. 2013).

85. Rodrigues et al., *supra* note 51, at 12.

be going nowhere and is constantly on the verge of implosion.⁸⁶ Other processes, such as the NTIA's facilitation of a multistakeholder process to develop a code of conduct on Mobile App Transparency, fared somewhat better, but even there the process was protracted and yielded a modest result.⁸⁷ The resulting code has drawn mixed reviews from the public.⁸⁸ Importantly, it is not yet clear which company (if any) will adopt it, what the consequences of noncompliance are, and to what extent it will change the reality on the ground.⁸⁹

DNT started as an advocacy group initiative, submitted during an FTC workshop on behavioral advertising in October 2007.⁹⁰ The group, led by the Center for Democracy and Technology, proposed: "To help ensure that [the privacy] principles are followed, the FTC should [c]reate a national Do Not Track List similar to the national Do Not Call List."⁹¹ The proposal would have required advertisers to submit their tracking domains to the FTC, which would make a DNT list available on its website for download by users who wish to limit tracking.⁹²

The idea remained dormant until July 2009, when privacy advocate Christopher Soghoian first developed his Targeted Advertising Cookie Opt-Out (TACO) mechanism as a prototype plug-in that automatically checks for a header

86. Omer Tene, *DNT 2.0: What Next for Policymakers?*, IAPP: PRIVACY PERSPECTIVES (Sept. 18, 2013), www.privacyassociation.org/privacy_perspectives/post/dnt_2.0_what_next_for_policymakers.

87. *Short Form Notice Code of Conduct to Promote Transparency in Mobile App Practices*, NAT'L TELECOMM. & INFO. ADMIN. (July 25, 2013), http://www.ntia.doc.gov/files/ntia/publications/july_25_code_draft.pdf.

88. One lawyer said, "It reads like guidance written by lawyers for lawyers. Even then, it's littered with so many caveats and exemptions about when the Code doesn't apply, it becomes almost impossible to read." *USA: NTIA App Privacy Code "Littered with Exemptions,"* DATAGUIDANCE, <http://dataguidance.com/news.asp?id=2079> (last updated January 8, 2013) (quoting Phil Lee, a partner at Field Fisher Waterhouse LLP). In a document titled "Head in the Digital Sand: How the Obama Administration's NTIA-led Multistakeholder Effort Doesn't Deliver its Promised Privacy Bill of Rights," privacy advocate Jeff Chester of the Center for Digital Democracy laid out a long list of alleged shortcomings of the NTIA process. *See generally* JEFF CHESTER, CTR. FOR DIGITAL DEMOCRACY, *HEAD IN THE DIGITAL SAND: HOW THE OBAMA ADMINISTRATION'S NTIA-LED MULTISTAKEHOLDER EFFORT DOESN'T DELIVER ITS PROMISED PRIVACY BILL OF RIGHTS* (Aug. 2013), *available at* <http://www.centerfordigitaldemocracy.org/sites/default/files/CDDPrivacyObamaAdmReportAugust2013.pdf>. Chester was quoted saying: "The NTIA [] should be nominated to run elections for the Kremlin[.] . . . They went from 'There's no consensus' to 'There is consensus that the document is final for now but can be changed in part based on testing.'" Katy Bachman, *Privacy Vote Sends Mixed Signals: No Consensus on Voluntary Code of Conduct for Apps*, ADWEEK (July 25, 2013, 6:51 PM), <http://www.adweek.com/news/technology/privacy-vote-sends-mixed-signals-151450>. *See also* Angeliqne Carson, *Did NTIA's Multi-Stakeholder Process Work? Depends on Whom You Ask*, IAPP: THE PRIVACY ADVISOR (Sept. 3, 2013), www.privacyassociation.org/publications/did_ntias_multi_stakeholder_process_work_depends_whom_you_ask.

89. Some would say that the NTIA is much less equipped to handle a multistakeholder process that organizations such as the IETF, W3C and ICANN, which have been around much longer and have policies, procedures, an infrastructure and a culture and a history of multistakeholder negotiations.

90. Ari Schwartz et al., *Consumer Rights and Protections in the Behavioral Advertising Sector*, CTR. FOR DEMOCRACY & TECH. (Oct. 31, 2007), www.cdt.org/privacy/20071031consumerprotectionsbehavioral.pdf; *What Does "Do Not Track" Mean? A Scoping Proposal by the Center for Democracy & Technology*, CTR. FOR DEMOCRACY & TECH. 1 (Jan. 31, 2011), www.cdt.org/files/pdfs/CDT-DNT-Report.pdf.

91. Schwartz et al., *supra* note 90 at 4.

92. *Id.*

on a website to determine whether to allow tracking cookies,⁹³ but the concept failed to resonate with the broader policy or advertising communities.⁹⁴ DNT first gained momentum as a viable policy concept on July 27, 2010, when FTC Chairman Jon Leibowitz testified at the Senate Committee on Commerce, Science, and Transportation on efforts to protect consumer privacy.⁹⁵ Departing from scripted remarks, Chairman Leibowitz stated that the FTC was calling for an industry-led DNT program.⁹⁶

Initial industry response was hardly enthusiastic, declaring that “[i]f mandated by the government, this would be tantamount to a government-sponsored, and possibly managed, ad-blocking program—something inimical to the First Amendment.”⁹⁷ DNT was seen as distraction from self-regulatory efforts organized by advertising industry groups, which were based on icons placed on behavioral ads and leading to opt-out tools.⁹⁸ However, the release of the FTC’s Preliminary Report in December 2010, which stated that “Commission staff supports a more uniform and comprehensive consumer choice mechanism for online behavioral advertising, sometimes referred to as ‘Do Not Track’” prompted the major browser makers to seriously engage with the DNT proposal.⁹⁹

93. Christopher Soghoian, *TACO 2.0 Released*, SLIGHT PARANOIA (July 27, 2009, 7:00 AM), <http://paranoia.dubfire.net/2009/07/taco-20-released.html>; Jeremy Kirk, *Privacy Add-ons Merged to Create Powerful Tool*, PCWORLD (June 15, 2010, 6:20 AM), http://www.pcworld.com/businesscenter/article/198852/privacy_addons_merged_to_create_powerful_tool.html; see Christopher Soghoian, *The History of the Do Not Track Header*, SLIGHT PARANOIA (Jan. 21, 2011, 4:00 PM), <http://paranoia.dubfire.net/2011/01/history-of-do-not-track-header.html> [hereinafter *History of DNT*].

94. *History of DNT*, *supra* note 93.

95. See *Consumer Online Privacy: Hearing Before the S. Comm. on Commerce, Sci., & Transp.*, 111th Cong. (2010) (testimony of Jon D. Leibowitz, Chairman, Fed. Trade Comm’n), available at http://commerce.senate.gov/public/index.cfm?p=Hearings&ContentRecord_id=0bfb9dfc-bbd7-40d6-8467-3b3344c72235&ContentType_id=14f995b9-dfa5-407a-9d35-56cc7152a7ed&Group_id=b06c39af-e033-4cba-9221-de668ca1978a&YearDisplay=2010.

96. Compare *id.*, with *Consumer Online Privacy: Hearing Before the S. Comm. On Commerce, Sci., & Transp.*, 111th Cong. (2010) (prepared statement of Jon D. Leibowitz, Chairman, Fed. Trade Comm’n), available at http://www.ftc.gov/sites/default/files/documents/public_statements/prepared-statement-federal-trade-commission-consumer-privacy/100727consumerprivacy.pdf.

97. *IAB Reviews Preliminary FTC Staff Report on Protecting Consumer Privacy*, INTERACTIVE ADVER. BUREAU (Dec. 1, 2010), www.iab.net/public_policy/1481209.

98. Colin O’Malley, *Self-Regulation Solves the Do Not Track Problem*, INTERACTIVE ADVER. BUREAU (Feb. 23, 2011, 4:57 PM), www.iab.net/iablog/2011/02/self-regulation-solves-the-do-not-track.html.

99. The content of this supporting footnote is adapted from Tene & Polonetsky, *supra* note 5, at 324-26: In December 2010, Microsoft implemented a “Tracking Protection” feature in its new Internet Explorer 9 browser, allowing users to select a Tracking Protection List (TPL) from a choice provided by various organizations, such as Abine, EasyList, PrivacyChoice, and TRUSTe. *IE9 and Privacy: Introducing Tracking Protection*, WINDOWS INTERNET EXPLORER ENGINEERING TEAM BLOG (Dec. 7, 2010, 1:10 PM), <http://blogs.msdn.com/b/ie/archive/2010/12/07/ie9-and-privacy-introducing-tracking-protection-v8.aspx>. While presented as an opt-in mechanism, TPL was really an opt-out tool (which users could choose to opt-into). Nick Wingfield & Julia Angwin, *Microsoft Adds Privacy Tool*, WALL ST. J., Mar. 15, 2011, at B1. Despite earlier skepticism about the concept, Microsoft also added a DNT browser header—which was automatically activated when a TPL (even an empty one) was uploaded—in its final release of Internet Explorer 9. *Id.* Mozilla, maker of the Firefox browser, presented an approach based on a DNT browser header. Aaron Brauer-Rieke, *“Do Not Track” Gains Momentum as Mozilla Announces New Tracking Tool*, CTR. DEMOCRACY & TECH. (Jan. 24, 2011), <https://www.cdt.org/blogs/aaron-brauer-rieke/%E2%80%9Cdo-not-track%E2%80%9D-gains->

In early 2011, W3C received a member submission from Microsoft proposing standardization of a DNT signal and tracking protection lists.¹⁰⁰ An April 2011 workshop on Web Tracking and User Privacy at Princeton University brought together almost a hundred participants from diverse backgrounds, out of which was chartered the Working Group.¹⁰¹ The Working Group was formed to “produce [r]ecommendation-track specifications for a simple machine-readable preference expression mechanism (‘Do Not Track’) and technologies for selectively allowing or blocking tracking elements,” and to “define the scope of the user preference and practices for compliance with it in a way that will inform and be informed by the technical specification.”¹⁰² Its success criteria were set forth as: “Production of stable Recommendation-track specifications”; and “Adoption of deliverables by user agents and compliance by industry.”¹⁰³

The initial Working Group meeting in Princeton already featured some of the persistent weaknesses that would continue to haunt W3C discussions, such as the inability to define the nature of the “tracking” that DNT protects users from, as well as peculiar decision-making processes.¹⁰⁴ For example, participants in the workshop voted on the appropriate definition of “tracking” through two “hum”

momentum-mozilla-announces-new-tracking-tool. In January 2011, Mozilla released Firefox 4, which allowed users to check a “Do Not Track” box in the “advanced” settings of the browser, prompting a header to be sent with every click or page request signaling to websites that the user does not wish to be tracked. *Mozilla Firefox 4 Beta, Now Including “Do Not Track” Capabilities*, MOZILLA BLOG (Feb. 8, 2011), <https://blog.mozilla.org/blog/2011/02/08/mozilla-firefox-4-beta-now-including-do-not-track-capabilities>. Unlike Microsoft’s TPL solution, the DNT header leaves it entirely up to receiving websites to honor the user’s request by omitting any tracking cookies from their response. *Privacy/Jan2011 DoNotTrack FAQ*, MOZILLAWIKI (last modified Jan. 24, 2011, 9:56 PM), https://wiki.mozilla.org/Privacy/Jan2011_DoNotTrack_FAQ. Google took a different approach, introducing the Keep My Opt-Outs plug-in, allowing users to permanently opt-out of online behavioral tracking by companies participating in self-regulatory programs. See Sean Harvey & Rajas Moonka, *Keep Your Opt-outs*, GOOGLE PUB. POL’Y BLOG (Jan. 24, 2011, 12:00 PM), <http://googlepublicpolicy.blogspot.com/2011/01/keep-your-opt-outs.html>. The new plug-in was meant to remedy the recurrent problem whereby users cleared out any opt-out cookies when purging their cookie folder, thus unknowingly re-entering the tracking domain. Harvey & Moonka, *supra*. Keep My Opt-Outs is itself cookie based—it deletes all cookies sent by registered domains and adds a DNT cookie for such domains. *Id.* Apple too added a DNT tool to a test version of its Safari browser included within the latest version of Lion, its new operating system. Nick Wingfield, *Apple Adds Do-Not-Track Tool to New Browser*, WALL ST. J., Apr. 14, 2011, at B5.

100. Andy Zeigler, Adrian Bateman, & Eliot Graff, *Web Tracking Protection: W3C Member Submission 24 February 2011*, WORLD WIDE WEB CONSORTIUM (Feb. 24, 2011), <http://www.w3.org/Submission/2011/SUBM-web-tracking-protection-20110224>.

101. *W3C Workshop on Web Tracking and User Privacy, Workshop Report*, WORLD WIDE WEB CONSORTIUM (Sept. 11, 2011), www.w3.org/2011/track-privacy/report.html [hereinafter *Workshop Report*].

102. *Tracking Protection Working Group Charter*, WORLD WIDE WEB CONSORTIUM (Sept. 25, 2013), www.w3.org/2011/tracking-protection/charter.html.

103. *Id.*

104. *Workshop Report, supra* note 101 (“Initially, regarding definitions of tracking, two ‘hum’ polls were taken. Among three choices for tracking—all tracking; tracking for online behavioral advertising; or some middle ground broad definition with certain exceptions (as in CDT’s or EFF’s proposals)—participants were fairly evenly divided on which proposal they would prefer to start with. Among the same set of choices, participants were also asked which would be a non-starter: while there were objections to the broad definition and the OBA-only definition, no one responded that the CDT-style proposal was an unacceptable starting point.”).

polls.¹⁰⁵ Addressing this method, one participant complained, “*There are billions of dollars at stake and the future of the Internet, and we’re trying to decide if one third-party is covered or didn’t hum louder!*”¹⁰⁶

The march of the Working Group is described in detail in a July 16, 2013, memorandum by Peter Swire, the Working Group’s co-chair at the time.¹⁰⁷ This Article is not intended to exhaustively document the Working Group’s deliberations, but rather to assess its (lack of) outcome as a test case for multistakeholder policymaking, in light of the claimed advantages of multistakeholder-driven self-regulation and co-regulation.

A. Expeditious Decision-Making

Pursuant to the preliminary workshop at Princeton in April 2011, the Working Group first met in September 2011 on the MIT campus in Cambridge, Massachusetts.¹⁰⁸ The First Public Working Drafts for both parts were published in November 2011.¹⁰⁹ Since then,¹¹⁰ the Working Group has conducted 105 teleconferences (typically lasting ninety minutes each) and met seven more times for multi-day face-to-face meetings, twice in Europe and the rest in the U.S., plus an additional meeting of the Global Considerations Task Force in Berlin.¹¹¹ In addition, it hosted a high-traffic mailing list and a web-based issue tracker.¹¹² The Working Group has seen the departure of two chairs as well as key staffers.¹¹³ It currently lists ninety-nine participants from forty-two organizations as well as seven “Invited Experts.”¹¹⁴ If participants agree on one thing, it is that the process was long, drawn out, and time consuming.¹¹⁵

The Working Group was originally chartered through July 2012.¹¹⁶ The

105. *Id.*

106. Telephone Interview with Anonymous Participant (Dec. 19, 2013) [hereinafter Anonymous Participant Interview (Dec. 19, 2013)].

107. *Explanatory Memorandum for Working Group Decision on “What Base Text to Use for the Do Not Track Compliance Specification,”* WORLD WIDE WEB CONSORTIUM (July 16, 2013), www.w3.org/2011/tracking-protection/2013-july-explanatory-memo [hereinafter *Base Text for DNT*].

108. See *Tracking Protection Working Group Charter*, *supra* note 102.

109. See Press Release, Ian Jacobs, World Wide Web Consortium, W3C Announces First Draft of Standard for Online Privacy (Nov. 14, 2011) (*available at* <http://www.w3.org/2011/11/dnt-pr.html.en>).

110. The numbers cited in this paragraph are updated through March 10, 2014.

111. See *Tracking Protection Working Group*, WORLD WIDE WEB CONSORTIUM, <http://www.w3.org/2011/tracking-protection> (last visited Mar. 10, 2014).

112. See *Issues*, WORLD WIDE WEB CONSORTIUM, www.w3.org/2011/tracking-protection/track/issues (last visited Feb. 15, 2014).

113. See Sam Pfeifle, *Is This the End for DNT? DAA Pulls Out of W3C Process*, IAPP: THE PRIVACY ADVISOR (Sept. 17, 2013), https://www.privacyassociation.org/publications/is_this_the_end_for_dnt_daa_pulls_out_of_w3c_process; Demedia, *Leadership Change at W3C’s Do Not Track Effort Reveals Lack of Online Industry Commitment to Protect Internet Privacy*, CTR. FOR DIGITAL DEMOCRACY (Nov. 28, 2012, 2:14 PM), <http://www.democraticmedia.org/leadership-change-w3c%E2%80%99s-do-not-track-effort-reveals-lack-online-industry-commitment-protect-internet>.

114. See *Participants in the Tracking Protection Working Group*, WORLD WIDE WEB CONSORTIUM (Sept. 16, 2013), www.w3.org/2000/09/dbwg/details?group=49311&public=1.

115. Mayer Interview, *supra* note 1; Anonymous Participant Interview (Dec. 19, 2013), *supra* note 106; Hanff Interview, *infra* note 139; Anonymous Participant Interview (Dec. 16, 2013), *infra* note 153; Verdi Interview, *infra* note 157; McNabb Interview, *infra* note 182.

116. See *Tracking Protection Working Group Charter*, *supra* note 102.

charter has been extended twice, currently running until April 2014.¹¹⁷ After more than two years of deliberations and failure to achieve its stated goals, it is safe to say that the Working Group did not obtain a result expeditiously. To be sure, the Working Group has been successful in fostering multistakeholder discussion (and garnering media attention).¹¹⁸ As Jonathan Mayer, a Stanford graduate student in computer science and law who participated in the process as an “invited expert” said, “*Where it has been successful is uncovering all of the possible issues surrounding the particular topic. It’s been very good at discussion, pulling out points of view, looking at how large the gap or divide may be.*”¹¹⁹

This is not stated cynically. An exchange of ideas, data, and proposals between various stakeholders in the Internet economy is a laudable goal, albeit not the Working Group’s purpose. Mayer stated,

*this notion—that groups that have had radically different views on major policy issues for a long time are going to sit down and negotiate for half a year or a year and come to some agreement that reconciles those views—it sounds like a pretty big stretch. Not impossible—you could imagine ways in which they were talking past each other, there were some misunderstandings, or some way of accommodating both visions—but unlikely.*¹²⁰

In what follows, this Part identifies several factors that hampered the Working Group’s quest for a swift resolution:

1. Decision-Making Rules

First and foremost, the Working Group’s rules for decision-making were not clear, leading to protracted and often circular discussions without an exit strategy. The W3C website states, “W3C Working Groups make decisions via consensus. In this context, consensus does not require unanimity, but majority votes are a last resort. The chairs are responsible for determining and recording consensus.”¹²¹ Yet, what does consensus mean in the context of the Working Group’s DNT discussions?¹²² Surely it cannot mean unanimity, which would embolden each and every participant to hold up an accord. But what, short of unanimity but stricter than simple majority, constitutes consensus?

117. *Id.*

118. See, e.g., Natasha Singer, *Do Not Track? Advertisers Say ‘Don’t Tread on Us’*, N.Y. TIMES, Oct. 14, 2012, at BU3, available at www.nytimes.com/2012/10/14/technology/do-not-track-movement-is-drawing-advertisers-fire.html; Somini Sengupta & Natasha Singer, *‘Do Not Track’ Rules Come a Step Closer to an Agreement*, N.Y. TIMES, July 16, 2013, at B3, available at www.nytimes.com/2013/07/16/technology/do-not-track-rules-for-advertising-to-web-users-come-a-step-closer-to-an-agreement.html; Claire Davenport, *‘Do Not Track’: Europe Wonders Why Tech Companies Are Dragging Their Feet*, HUFFINGTON POST, (Oct. 10, 2012), www.huffingtonpost.com/2012/10/10/do-not-track-europe_n_1955713.html; *Don’t Keep on Trackin’*, ECONOMIST BABBAGE BLOG (May 26, 2012), www.economist.com/blogs/babbage/2012/05/online-advertising.

119. Mayer Interview, *supra* note 1.

120. *Id.*

121. *Tracking Protection Working Group—Frequently Asked Questions*, WORLD WIDE WEB CONSORTIUM, www.w3.org/2011/tracking-protection/faq (last visited Feb. 15, 2014).

122. See *W3C Process Document, 3.3 Consensus*, WORLD WIDE WEB CONSORTIUM, www.w3.org/2005/10/Process-20051014/policies#Consensus (last visited Feb. 15, 2014).

Several participants complained that not only were the rules of engagement unclear from the start, but they were also changed frequently throughout the process. Mayer said that

*the rules pretty much changed depending on the time and depending on whom you asked. To hear the chairs tell it early on, there needed to be agreement across at least three broad stakeholder views: the companies that were tracking users (advertising, analytics, social and so on), the web browsers, and the participants who roughly represented user concerns. If you want to slice and dice a little more finely, you might say something like, we will break out advertising, analytics, and social; we might break out big versus small companies; then web browsers; then maybe we break out activists versus researchers versus policymakers. But some rough notion of buckets, and you had to get agreement from all of these.*¹²³

Clearly, participants did not know which stakeholders needed to sign off on a deal before consensus was announced. And whereas “hum” polls were accepted for determining consensus early on in the process, some decisions were later made via online voting, where supporters of a proposition vote “+1” and opponents “-1.”¹²⁴ This implies a simple majority rule, quite distant from the consensus-based model anticipated by some of the participants.

2. Representation and Composition

The requisite voting majority touches on the related issue of representation. Formal policymaking processes are typically run according to clear rules of representation.¹²⁵ The fact that there are as many representatives from Delaware in the Senate as there are from Texas could conceivably be controversial, but it is grounded in rules written into the Constitution.¹²⁶ In top-down regulation, elected officials or regulators whom they appoint are the ones driving policymaking, providing a degree of public representation and accountability.¹²⁷ Yet, when it comes to self- or co-regulatory multistakeholder processes, equitable representation norms are fickle.

Whom are Working Group participants representing? For example, did Mayer, the Stanford PhD student and privacy advocate who joined the Working Group as an “invited expert,” represent 2.5 billion Internet users or just himself? Or perhaps something in between, such as all Internet users who live in Palo Alto and own a Mac? Similarly, among the many industry participants, should votes be weighed by consumer base, market share or some other criteria, or should Google’s vote be equal to that of a small online ad intermediary? Clearly, if the votes are not weighed, but rather tallied by show of hands, the composition of the Working Group becomes determinative. Indeed, “packing” the Working Group with as

123. Mayer Interview, *supra* note 1.

124. See, e.g., *Draft Minutes from Tracking Protection Working Group Teleconference*, WORLD WIDE WEB CONSORTIUM (June 19, 2013), www.w3.org/2013/06/19-dnt-minutes.

125. See generally Kenneth W. Abbott & Duncan Snidal, *Why States Act Through Formal International Organizations*, 42 J. CONFLICT RESOL. 3 (1998).

126. U.S. CONST. art. I, § 3.

127. See generally William F. West, *Formal Procedures, Informal Processes, Accountability, and Responsiveness in Bureaucratic Policy Making: An Institutional Policy Analysis*, 64 PUB. ADMIN. REV. 66 (2004).

many allies as possible can ensure a desirable result.

Packing the Working Group was possible, though costly, given that participation fees amounted to more than \$68,000 for large companies,¹²⁸ \$7,900 for small and medium size companies and large NGOs,¹²⁹ and \$2,250 for small enterprises with less than 10 employees.¹³⁰ Some advocates argued that the strategy for industry was to pay for as many participants as possible, sometimes resulting in industry groups overlapping with their constituents.¹³¹ For example, the DAA attended the Working Group together with its constituent industry groups, the American Association of Advertising Agencies (4A's), Direct Marketing Association, Interactive Advertising Bureau, and NAI, as well as multiple corporate members of these groups.¹³² In this context it was not always clear whether, on any given issue, an industry group represented all of its members, a majority thereof, or perhaps only itself.

Mayer argued that the imperative for industry was not to pack the Working Group so as to assure *passage* of resolutions, but rather to *prevent* any resolution that may be damaging. In his words,

*One strategic call that advertising groups made—that I think was a very good call for their part—was to try to pack the group, to try to get as many people in. Not necessarily because they thought they could get anything done that way, but because they thought it would make it really, really hard for the group to ever come to any sort of agreement that they disagreed with.*¹³³

While advocates argued that the Working Group was dominated by industry, some industry participants claimed that the protracted discussions, necessary travel, and substantial participation fee meant that the group was captured not by the industry as a whole, but rather by a small subset consisting of large, multinational corporations.¹³⁴ Small- and medium-sized enterprises, which make up a large portion of the Internet economy, particularly in areas still vibrant with entrepreneurship and growth, were thus underrepresented and greatly disadvantaged. Not only would they have to invest the high participation fee, but they would also need to expend human resources to attend the meetings and follow the discussion.

The only Working Group participants exempt from participation fees were

128. Defined as: “For-profit organization that has annual gross revenue, as measured by the most recent audited statement, of greater than or equal to 50,000,000 USD.” *Membership Fees – W3C: Fee Table for United States*, WORLD WIDE WEB CONSORTIUM, www.w3.org/Consortium/fees?countryCode=US&quarter=01-01&year=2014#results (last visited Mar. 14, 2014).

129. Defined as: “All other organizations, including non-profit organizations and government agencies.” *Id.*

130. Defined as: “Enterprises and non-profits with 10 or fewer employees, who are not also membership organizations, revenues less than 3,000,000 USD and have never been a W3C Member.” *Id.*

131. Mayer Interview, *supra* note 1.

132. See *Participants in the Tracking Protection Working Group*, WORLD WIDE WEB CONSORTIUM (Sept. 16, 2013), <http://www.w3.org/2000/09/dbwg/details?group=49311&public=1&order=org>.

133. Mayer Interview, *supra* note 1.

134. One participant noted that the W3C itself is industry funded. Anonymous Participant Interview (Dec. 19, 2013), *supra* note 106.

those admitted by the chairs as “invited experts.”¹³⁵ Currently, this group, whose selection criteria remain opaque,¹³⁶ comprises seven such “invited experts,” including three privacy advocates (Jeffrey Chester, John Simpson, and Walter van Holst), two academics (Edward Felten and Paul Ohm), a European academic-regulator (Rob van Eijk), and a libertarian think tanker (Berin Szoka). In terms of opportunity costs, even without participation fees, the burden on civil society representatives was heavy. Privacy advocates had to spend their time and effort *gratis* in dozens of meetings and web forums, while industry lawyers and lobbyists were paid to represent their companies in the same discussions.¹³⁷ Mayer added, “*The opportunity costs look very, very different and the ability to marshal resources also.*”¹³⁸

3. Delay Tactics

One advocate, Alexander Hanff, argued that regardless of procedural rules, the deck was stacked against civil society given that a good result for industry would be for the Working Group to achieve no result at all.¹³⁹ He claimed that during the protracted discussions, industry could continue to run rampant using any available and newly developed tracking technologies and capabilities.¹⁴⁰ To stop the snowball effect, civil society needed a clean “victory,” while industry’s best strategy was to stall, pushing back deadline after deadline, while continuing to track users.¹⁴¹ In his view, a potential win for civil society could only occur through the judicial system or the court of public opinion,¹⁴² not via a multistakeholder process.¹⁴³

Mayer said,

*[There were] myriad ways of delaying within the W3C process. It’s trivial to re-raise an issue that’s been discussed for years. It’s almost laughable. The stuff that people were talking about even before the W3C process is the very same stuff we’re talking about today. It’s kind of like circling the drain but never actually going down it. And so it’s really easy to continue to have those endless discussions.*¹⁴⁴

This approach, however, depicts industry as a monolith whose interest is to avert regulation. In reality, industry comprises a plethora of voices, including

135. For a definition of “invited expert,” see *Invited Expert and Collaborator Agreement*, WORLD WIDE WEB CONSORTIUM, <http://www.w3.org/Consortium/Legal/2007/06-invited-expert> (last visited Apr. 21, 2014).

136. See *Instructions for non-Members (Invited Experts)*, WORLD WIDE WEB CONSORTIUM, <http://www.w3.org/2004/08/invexp> (last visited Mar. 14, 2014).

137. Mayer Interview, *supra* note 1.

138. *Id.*

139. Interview with Alexander Hanff, privacy advocate, in Brussels, Belg. (Dec. 11, 2013) [hereinafter Hanff Interview].

140. *Id.*

141. *Id.*

142. See, e.g., Alan Travis, *ID Cards Scheme to be Scrapped within 100 Days*, THE GUARDIAN, May 27, 2010, 10:16 PM, <http://www.theguardian.com/politics/2010/may/27/theresa-may-scrapping-id-cards>.

143. Hanff Interview, *supra* note 139.

144. Mayer Interview, *supra* note 1.

factions that compete vigorously against one another.¹⁴⁵ Indeed, some industry participants said that their biggest concern throughout the process was not the engagement with consumer advocates, but rather the power play between companies trying to cement a competitive advantage via a global technology standard while W3C remains on the sidelines.

4. *The Role of the Chair*

In any policymaking process, the role of the chair is key both in terms of agenda setting and decision-making.¹⁴⁶ Clearly, if the chair could break deadlock and force a decision over the objection of some of the participants, he or she would have the power to drive the process forward. Yet, in the case of the Working Group, the chair lacked formal decision-making authority and acted more as a facilitator.¹⁴⁷ Importantly, the chair's responsibilities did not include drafting the deliverables, a task assigned to designated "editors."¹⁴⁸ In addition, from the outset, the Working Group operated with two (currently three) co-chairs—in and of itself a mode that weakens the chair's role.¹⁴⁹

Initially, the Working Group appointed two chairs: Matthias Schunter (first with IBM and now Intel) led the development of the Tracking Preference Expression Specification, which defines the technical mechanisms for expressing a DNT preference; and Aleecia McDonald (first Mozilla and now Stanford) led the development of the Tracking Compliance and Scope Specification, which defines the meaning of a DNT preference and sets out practices for websites to comply with this preference.¹⁵⁰ In November 2012, Peter Swire (first Ohio State and now Georgia Tech) succeeded McDonald as the co-chair for the compliance specification.¹⁵¹ Swire, in turn, departed in August 2013 to join the President's Review Group on Intelligence and Communications Technologies.¹⁵² When asked about the chair's selection process, one participant said,

They just come up with the name, there is no process. They give you no transparency into who was considered, why various candidates were not considered, or why they ultimately were not asked—or even those that were asked and then politely rejected the offer. There was no transparency into any of that

145. This is an area where the first-party and third-party distinction made a big difference. For some of the intricacies of the still unresolved first-party/third-party distinction, see issues 9, 10, 49, 50, 54, 59, 66, 72, 73, 77, 91, 123, 137, 140, 154, 159 and 203 in *Issues*, WORLD WIDE WEB CONSORTIUM, <http://www.w3.org/2011/tracking-protection/track/issues> (last visited Mar. 14, 2014).

146. See, e.g., Jonas Tallberg, *The Power of the Chair: Formal Leadership in International Cooperation*, 54 INT'L STUD. Q. 241 (2010).

147. See *W3C Process Document*, WORLD WIDE WEB CONSORTIUM, <http://www.w3.org/2005/10/Process-20051014/policies.html> (last visited Mar. 14, 2014).

148. See *W3C Editors' Home Page*, WORLD WIDE WEB CONSORTIUM, <http://www.w3.org/2003/Editors> (last visited Mar. 14, 2014).

149. See *Tracking Protection Working Group Charter*, *supra* note 102.

150. See *Base Text for DNT*, *supra* note 107.

151. *Id.*

152. Peter Swire, *My Appointment to President's Review Group, and Resignation as Co-Chair*, WORLD WIDE WEB CONSORTIUM (Aug. 27, 2013), <http://lists.w3.org/Archives/Public/public-tracking/2013Aug/0024.html>.

*process; it was just a name delivered at the end of the day.*¹⁵³

Several Working Group participants noted that during McDonald's term, the role of the chair was viewed as an enabler of discussion, in charge of helping bridge differences between the different factions. In the words of a participant, "*the chair was otherwise a first among equals, just another voice in the group.*"¹⁵⁴ Swire, on the other hand, sought to be more proactive, but his quest too fell flat amid a storm of allegations, with multiple participants questioning the source of his authority to substitute his own judgment for that of the Working Group.¹⁵⁵ Referring to the chairs' efforts, Mayer said, "*There were many, many people from advertising companies and advocacy groups who were just unhappy across the board because of this notion that 'hey, the chairs are wonderful, but what special legitimacy do they have to decide how the rules of the road should go on web browsers?'*"¹⁵⁶

5. Drafting a Straw Man

A related issue concerns the identity and role of the party "holding the pen." To prevent endless discussion, particularly of issues with complex social, economic and even philosophical dimensions, such as those implicated in DNT, someone must ground the debate in a straw man document, which can be thoroughly edited and even replaced during the process.¹⁵⁷ As Mayer said, "*The factual exploration is great, and it's a necessary predicate to the work getting done, but we want to make sure people remember that it's a predicate; it's not the goal.*"¹⁵⁸ In multistakeholder processes organized by the FTC and California Attorney General,¹⁵⁹ it was evident that regardless of stakeholder input, the regulator held the pen. Despite the NTIA not itself holding enforcement powers, even that process was channeled to a document written by the organizer itself.¹⁶⁰ Conversely, the Working Group discussions ran rampant without a backstop, as even the chairs were unauthorized to crystalize the discussion into a compromise text.¹⁶¹

153. Telephone Interview with Anonymous Participant (Dec. 16, 2013) [hereinafter Anonymous Participant Interview (Dec. 16, 2013)].

154. Mayer Interview, *supra* note 1.

155. Katy Bachman, *Turmoil Surfaces in the Do Not Track Group, Process Disagreement May Derail Consensus*, ADWEEK, July 19, 2013, <http://www.adweek.com/news/technology/turmoil-surfaces-do-not-track-group-151307>.

156. Mayer Interview, *supra* note 1.

157. Telephone Interview by Kelsey Finch with John Verdi, Dir. of Privacy Initiatives, Nat'l Telecomm. & Info. Admin. (Dec. 5, 2013) [hereinafter Verdi Interview].

158. Mayer Interview, *supra* note 1.

159. Kamala D. Harris, Att'y Gen., Cal. Dep't of Justice, *Privacy on the Go: Recommendations for the Mobile Ecosystem* (Jan. 2013), http://oag.ca.gov/sites/all/files/pdfs/privacy/privacy_on_the_go.pdf.

160. *Privacy Multistakeholder Process: Mobile Application Transparency*, NAT'L TELECOMM. & INFO. ADMIN. (Nov. 12, 2013), <http://www.ntia.doc.gov/other-publication/2013/privacy-multistakeholder-process-mobile-application-transparency>.

161. See *public-tracking@w3.org Mail Archives*, WORLD WIDE WEB CONSORTIUM, <http://lists.w3.org/Archives/Public/public-tracking/#latest> (last visited Mar. 14, 2014) (indicating over 9,000 participant comments to date); *Tracking Protection Working Group Issue Tracking*, WORLD WIDE WEB CONSORTIUM, <http://www.w3.org/2011/tracking-protection/track/issues> (last visited Mar. 14, 2014) (indicating 242 issues listed to date); *W3C Process Document*, *supra* note 147.

6. Web-Based Communications Tools

Another potentially complicating factor for the discussion was the Working Group's use of an official backchannel, an active email listserv for debating the open issues.¹⁶² Mayer explained that the online discussions “*had a tendency to get a little vitriolic at times, where it wasn't even meant that way it was just that—as anyone who sends email knows—it's super easy to misunderstand the tone someone uses.*”¹⁶³ Some participants stated they felt obliged to be constantly engaged on the backchannel to immediately refute any position they disagreed with lest others assume they concurred.¹⁶⁴

John Verdi of the NTIA, which had no official backchannel, noted “*we wanted to keep the process as open as possible, so what happened in the room was the official record; this kept everyone on the same page, and we didn't have people saying 'oh, I raised this on the list' or 'I opened this issue on the backchannel.'*”¹⁶⁵ He added that, “*remote participation is challenging to get right, but important to provide. No geographic location has a monopoly on expertise, so we need to do the best we can to enable participation from stakeholders outside DC.*”¹⁶⁶

Mayer noted that towards the last stages of the process, there was a sense that a deal may be being negotiated behind the scenes where not everyone had a voice. He stated:

*That rankled a bunch of folks in the group. And this came out through the framework and drafts and so on that were getting pitched—these documents seemingly came out of nowhere. But clearly they came out of some backroom talks between certain groups of stakeholders. That was really uncomfortable.*¹⁶⁷

The Working Group used another web-based communication resource—an issue tracker intended to capture and contain the open and closed topics for discussion.¹⁶⁸ Alas, use of this tool became daunting, given that the Working Group was unable to close an issue without at the same time opening several more, whether duplicative, linked, or entirely independent.¹⁶⁹ Instead of streamlining the discussion and stimulating progress, the issue tracker contributed to a chaotic environment and facilitated what some participants characterized as filibuster tactics.¹⁷⁰ Conceivably, if the chairs controlled the list of open issues, the issue tracker could have been conducive to progress. Yet, as discussed above, the Working Group chairs were not perceived as empowered to even decide whether an issue remains outstanding or not.¹⁷¹

162. See *public-tracking@w3.org Mail Archives*, *supra* note 161.

163. Mayer Interview, *supra* note 1.

164. Anonymous Participant Interview (Dec. 16, 2013), *supra* note 153.

165. Verdi Interview, *supra* note 157.

166. *Id.*

167. Mayer Interview, *supra* note 1.

168. See *Issues*, WORLD WIDE WEB CONSORTIUM, <http://www.w3.org/2011/tracking-protection/track/issues> (last visited Mar. 22, 2014) (currently listing in excess of 240 issues).

169. See *Tracking Protection Working Group Issue Tracking*, *supra* note 161.

170. Mayer Interview, *supra* note 1.

171. See *supra* Part IV.A.4.

B. Informed by Industry Knowledge and Expertise

One of the main perceived virtues of multistakeholder policymaking is the ability to draw on the knowledge and expertise of multiple parties from various parts of the ecosystem. This is only true, however, if the parties can agree on the facts. In the DNT context, this was not typically the case. Quite the contrary, Working Group participants consistently sparred over basic concepts, terms, and definitions, such as the level of data collection required to ensure basic online functionality.¹⁷² Indeed, after more than two years of deliberations, the Working Group has not yet been able to define many of the fundamental terms underlying a tracking protection policy, not least the meaning of “tracking” itself.¹⁷³ As Swire noted in the Chair’s Explanatory Memorandum, “Defining the term ‘tracking’ is obviously an important aspect of defining the meaning of ‘Do Not Track.’”¹⁷⁴

1. Arguing over Facts

Consider, for example, data de-identification.¹⁷⁵ A deep rift separated the position of several “invited experts,” such as Edward Felten (Princeton) and Jonathan Mayer (Stanford), from those of industry voices such as Shane Wiley (Yahoo).¹⁷⁶ While Wiley argued that hashing unique identifiers would be sufficient to separate data from real world identities, Felten and Mayer believed that as long as such pseudonymized data could be re-identified, it must be viewed as personal.¹⁷⁷ As Mayer said, “we’d have these radically different views—radically different technical views, not just talking policy implications. There was just no way of reconciling them. The W3C had no way of saying ‘okay, pony up with your technical experts.’”¹⁷⁸ Hence, the disagreements were not over policy or legal interpretation, but rather around *the facts*. In the words of Albert Einstein, “If the facts don’t fit the theory, change the facts.”¹⁷⁹

2. Engineers vs. Lawyers

Some participants lamented the steady shift of the Working Group makeup from a tight-knit engineering clique to a group dominated by lawyers and government relations professionals.¹⁸⁰ This is not surprising, given that the issues

172. See David Goldman, *Do Not Track Proposal Is DOA*, CNNMONEY, July 16, 2013, 1:47 PM, <http://money.cnn.com/2013/07/16/technology/do-not-track>.

173. Other crucial concepts that remain elusive are “de-identified data,” the distinction between “first-” and “third-parties,” “permitted uses,” and more. See *Tracking Compliance and Scope*, WORLD WIDE WEB CONSORTIUM (Jan. 27, 2014), <http://www.w3.org/2011/tracking-protection/drafts/tracking-compliance.html#scope-and-goals>.

174. See *Base Text for DNT*, *supra* note 107.

175. *Issue-188: Definition of De-Identified (Or Previously, Unlinkable) Data*, WORLD WIDE WEB CONSORTIUM, <http://www.w3.org/2011/tracking-protection/track/issues/188> (last visited Mar. 22, 2014).

176. See, e.g., E-mail from Shane Wiley, Yahoo, to Dan Auerbach, EFF (Oct. 23, 2012) (available at <http://lists.w3.org/Archives/Public/public-tracking/2012Oct/0447.html>).

177. *Id.*

178. Mayer Interview, *supra* note 1.

179. Attributed. See BRAINYQUOTE, <http://www.brainyquote.com/quotes/quotes/a/alberteins136887.html> (last visited Mar. 22, 2014).

180. Doty & Mulligan, *supra* note 2, at 153-54.

on the agenda cut to the core of high stakes business and social policy considerations. In medieval days, a discussion among scientists would cease to be purely scientific when the existence of god became an issue. At that point, the bishops would rush into the room. Similarly, when Working Group discussions became fraught with business and policy implications, the nature of the discussants' expertise shifted as well.¹⁸¹

One complication participants noted about dealing with lawyers and government affairs professionals is that they may not have sufficient technical expertise. Joanne McNabb, Director of Privacy Education and Policy at the California Attorney General's Office, who participated in the process run by her office, said:

*[Lawyers and government affairs professionals] don't have the actual knowledge that you need, so they have to keep going back, back, back. We made an effort to get people who are not only with this particular stakeholder but also have the operational or more direct knowledge of what the issue is. And, at the very least, to encourage the government affairs representatives, if they're the ones who end up coming, to go back and get to the people who are actually going to have the substantive knowledge and get them engaged.*¹⁸²

In addition, some participants thought that as a matter of professional ethos, engineers viewed the issues as problems to solve, while government affairs and legal experts were less likely to come to agreement.¹⁸³

C. Fostering Collaboration and Compliance

Proponents of a multistakeholder process claim that rules negotiated by the industry are more likely to foster implementation and compliance. Instead, the Working Group discussions increasingly became more polarized and accompanied by a constant drumbeat of warnings that industry players would vote with their feet and ignore any result that came short of their expectations.

1. Good Spec; No Implementation

This dire prediction resonates in light of the historical example of another W3C foray into policymaking, the Platform for Privacy Preferences (P3P) standard issued in 2002.¹⁸⁴ P3P was conceived as a standard allowing users and websites to match privacy policies through machine-readable code.¹⁸⁵ Specifically, P3P would enable machine-readable privacy policies that could be retrieved automatically by web browsers or other user agents.¹⁸⁶ The browser would then compare each

181. *Id.*

182. Telephone Interview with Joanne McNabb, Dir. Privacy Educ. & Policy, Cal. Att'y Gen. Office (Dec. 15, 2013) [hereinafter McNabb Interview].

183. *Id.*

184. Lorie Cranor et al., *The Platform for Privacy Preferences 1.0 (P3P1.0) Specification, W3C Recommendation*, WORLD WIDE WEB CONSORTIUM (Apr. 16, 2002), <http://www.w3.org/TR/P3P>.

185. *See id.*; Ari Schwartz, *Looking Back at P3P: Lessons for the Future*, CTR. FOR DEMOCRACY & TECH. (Nov. 2009), http://www.cdt.org/files/pdfs/P3P_Retro_Final_0.pdf.

186. *Platform for Privacy Preferences (P3P) Project, Enabling Smarter Privacy Tools for the Web*, WORLD WIDE WEB CONSORTIUM (Nov. 20, 2007), <http://www.w3.org/P3P>.

policy against a user's privacy preferences and assist the user in deciding when to exchange data with a website or deploy additional features, such as user alerts or cookie blockers.¹⁸⁷

To discuss implementation, the W3C set up a working group, which embarked on a long and laborious process spanning almost a decade.¹⁸⁸ Lorrie Cranor, who led the discussions, compared the process to “an out-of-control construction on a kitchen that at first only needs a small new appliance (a toaster) but ends up with a plan for new cabinets, floors and lighting.”¹⁸⁹ On the one hand, privacy advocates opposed P3P on the grounds that industry groups were using it “as an excuse to delay the progress of genuine enforceable privacy rights in the US”,¹⁹⁰ the European Article 29 Working Party voiced similar concerns.¹⁹¹ On the other hand, industry viewed the emerging standard with suspicion, concerned about excessive transparency and the potential impact on business practices.¹⁹²

After initial roll out, P3P appeared to have a “chicken and egg” problem: P3P policies would not be created until there was implementation by a widely used web browser, but browser implementation would not do anything until there were policies online.¹⁹³ Microsoft's Internet Explorer was the only major browser to adopt P3P, and it continues to do so to this day.¹⁹⁴ However, most Internet Explorer users remain completely unaware of P3P.¹⁹⁵ Worse, thousands of websites, including some of the web's most popular sites, “post bogus P3P ‘compact policies’ that circumvent the default P3P-based cookie-blocking system in Internet Explorer.”¹⁹⁶

In many ways, the Working Group effort to standardize DNT is reminiscent of the P3P fiasco. As Mayer said, “*At the end of the day, if you come out with something that only one company wants to implement—and this is an understood, voluntary process—then hopefully the collective should understand that it was a failure.*”¹⁹⁷

187. *The Platform for Privacy Preferences 1.0 (P3P1.0) Specification*, WORLD WIDE WEB CONSORTIUM (Apr. 16, 2002), <http://www.w3.org/TR/P3P>.

188. The W3C started its work on P3P in 1997 and the P3P Specification Working Group was chartered in July 1999.

189. See Schwartz, *supra* note 185, at 3.

190. Cranor et al., *supra* note 184.

191. WORKING PARTY 11, WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA, OPINION 1/98: PLATFORM FOR PRIVACY PREFERENCES (P3P) AND THE OPEN PROFILING STANDARD (OPS) (June 16, 1998), available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/1998/wp11_en.pdf.

192. See, e.g., Fran Maier, *More on the Problem with P3P*, TRUSTE BLOG, Sept. 14, 2010, <http://www.truste.com/blog/2010/09/14/more-on-the-problem-with-p3p>.

193. Schwartz, *supra* note 185, at 8 (“Either the market will work or direct regulation will dictate the value for the companies, or the idea will fail, but in no case is it possible for the developers of a concept like P3P to create critical mass of acceptance among Web sites.”).

194. *Privacy in Internet Explorer*, WINDOWS DEVELOPER NETWORK, <http://msdn.microsoft.com/en-us/library/ms537343.aspx> (last visited Mar. 22, 2014).

195. Lorrie Faith Cranor, *Necessary but Not Sufficient: Standardized Mechanisms for Privacy Notice and Choice*, 10 J. TELECOMM. & HIGH TECH. L. 273, 281 (2012).

196. Lorrie Cranor, *P3P is Dead, Long Live P3P!*, THIS THING, Dec. 3, 2012, <http://lorrie.cranor.org/blog/2012/12/03/p3p-is-dead-long-live-p3p> (emphasis added).

197. Mayer Interview, *supra* note 1.

2. Incentive to Comply?

What is the incentive on the part of industry to adopt a standard produced through a multistakeholder process? If multistakeholder input is sought as part of a formal process of top-down regulation, such as in notice and comment rulemaking, industry will engage in order to influence the resulting framework. If negotiations take place against a backdrop of binding legislation, industry could be in it to benefit from an enforcement safe harbor or clearer statutory guidance.

The NTIA process is a hybrid between a “quasi voluntary” discussion with a regulator, such as the FTC or California Attorney General, and a purely voluntary process, such as the Working Group. On the one hand, the NTIA does not have enforcement powers and cannot impose a compromise. On the other hand, a process orchestrated by the U.S. government is likely to command close attention from the industry. The fear, which some think materialized,¹⁹⁸ is that an accord reached in these circumstances—obligatory participation but little enforcement prospect—will be vague or narrow in scope and not command a large following.

The dynamic is very different in the context of the Working Group, which operates in the absence of existing regulation. Here, stalling tactics come at *no cost*, and the process could ostensibly continue forever.

3. External Disruptions

Despite all of the shortcomings discussed above, the Working Group would have been in relatively good shape had it not been for several exogenous disruptions. All of the participants interviewed, including both privacy advocates and industry representatives, pointed to Microsoft’s August 2012 decision to switch DNT on by default in Internet Explorer¹⁹⁹ as a cataclysmic event for the Working Group.²⁰⁰ After that, the process spiraled out of control and focused on struggling to keep the stakeholders at the table. An additional blow came in February 2013, when Mozilla announced it would set Firefox browsers to automatically block third-party cookies.²⁰¹

The move by Microsoft, whose various versions of Internet Explorer continue to command more than 50% of the desktop market,²⁰² was particularly significant, because the industry recoiled from any contemplated compromise. Industry representatives were prepared to negotiate the specifics of an opt-out tool, realizing

198. See *supra* text accompanying note 88.

199. Brendon Lynch, *Do Not Track in the Windows 8 Setup Experience*, MICROSOFT ON THE ISSUES, Aug. 7, 2012, 10:00 AM, http://blogs.technet.com/b/microsoft_on_the_issues/archive/2012/08/07/do-not-track-in-the-windows-8-set-up-experience.aspx; see also Ryan Singel, *In Ad Network Nightmare, Microsoft Making ‘Do Not Track’ Default for IE 10*, WIRED, May 31, 2012, 8:04 PM, <http://www.wired.com/threatlevel/2012/05/ie10-do-not-track>.

200. Mayer Interview, *supra* note 1; Anonymous Participant Interview (Dec. 19, 2013), *supra* note 106; Hanff Interview, *supra* note 139; Anonymous Participant Interview (Dec. 16, 2013), *supra* note 153; Verdi Interview, *supra* note 157; McNabb Interview, *supra* note 182.

201. Gregg Keizer, *Firefox to Auto-Block Third-Party Ad Cookies by Summer*, COMPUTERWORLD, Feb. 25, 2013, 6:40 AM, http://www.computerworld.com/s/article/9237105/Firefox_to_auto_block_third_party_ad_cookies_by_summer.

202. See *Desktop Browser Version Market Share (February 2014)*, NETMARKETSHARE.COM, <http://www.netmarketshare.com/browser-market-share.aspx?qprid=2&qpcustomd=0>.

that the majority of users would not tamper with the default.²⁰³ The implications of a major browser automatically opting-out users were grim for any business operating in the online advertising space. Industry, thus, retrenched and acted as if it was fighting for survival.²⁰⁴ Referring to Microsoft's move, one participant remarked, "*The trust was gone. There was no trust left. They'd been in the process for a year agreeing on default off, and then unilaterally made this massive public statement to gain their own competitive advantage against Google and others.*"²⁰⁵

Mayer suggested, however, that major external events could conceivably serve as a catalyst for concessions:

*When it looked like Microsoft's decision to enable DNT by default in a beta version of Internet Explorer was going to potentially jeopardize negotiations, advocates suddenly made some concessions. And when it looked like companies were going to start cracking down on technical countermeasures—browser companies, too—there were some hints of concessions out of the ad industry. So, W3C provides the forum, but it was things outside of W3C that moved the needle on how close to an agreement we were.*²⁰⁶

Microsoft's announcement was not the only external event to rock the boat. Other notable disruptions were caused by change of personnel, including two of the chairs, as well as the decision of the DAA to leave the process.²⁰⁷ And while such developments are not unexpected in the context of a process that lingers for years, they clearly did not improve the odds for the Working Group to reach an accord.

V. CONCLUSION

Profound technological changes and shifting social norms have forced privacy policymakers to chase a rapidly moving target. This has led government and regulatory agencies to coopt industry and civil society representatives in search of self- or co-regulatory models based on multistakeholder discourse. The purported advantages of multistakeholder policymaking abound and include fact- and experience-based deliberations, expeditious results, and enhanced implementation and compliance. This Article assesses why one such process, the W3C quest to standardize DNT, failed to deliver along these vectors. Instead, W3C's efforts featured protracted discussions not leading to tangible results, erratic decision-making processes, persistent disagreement over facts, and gloomy predictions about the prospects of implementation should a standard arise.

Based on a series of interviews with participants in the process, including leading industry, civil society, and government voices, this Article identifies shortcomings in the Working Group process, including the absence of clear rules of

203. See, e.g., E-mail from Mike Zaneis, Interactive Adver. Bureau, to Jeffrey Chester, Ctr. for Digital Democracy (July 26, 2012) (available at <http://lists.w3.org/Archives/Public/public-tracking/2012Jul/0153.html>).

204. *Id.*

205. Anonymous Participant Interview (Dec. 19, 2013), *supra* note 106.

206. Mayer Interview, *supra* note 1.

207. See Aaron Taube, *Advertising Group Pulls Out of Internet Tracking Negotiation*, BUS. INSIDER, Sept. 17, 2013, 11:54 AM, www.businessinsider.com/ad-industry-leaves-do-not-track-negotiations-2013-9.

engagement, soft deadlines and a vague definition of deliverables, constrained chairs with little decision-making power, and potentially unbalanced representation.

These shortcomings do not necessarily imply that multistakeholder processes are fundamentally flawed. As a vehicle for self- or co-regulation, they should not be judged in a vacuum, but rather against alternative rulemaking processes. Given the gridlock in Washington and Brussels, multistakeholder processes may yet bring more promise to policymaking in the privacy space than any tangible alternative. Moreover, this Article does not assert that *every* multistakeholder policymaking process is destined to end like DNT. Some of the failings of the Working Group, such as unclear rules of representation, may be endemic to multistakeholder processes; others, such as pay-to-play obligations and a backchannel for discussion, may be more specific to the W3C, or even the alignment of forces within the Working Group.

However, to avoid evident pitfalls, multistakeholder processes should: 1) be structured around manifest and achievable goals; 2) set forth clear procedures for voting, decision-making, and consensus; 3) devise rational, fair rules of representation, taking into account the relative costs and benefits and access to resources that various stakeholders have; 4) seek to coalesce around straw man documents as early as possible in the process; 5) empower a chair or editor to express decisions in writing; and 6) optimally operate under a backstop of formal rulemaking, which will reduce any incentive to stall. In short, with firm structure and strong leadership, multistakeholder processes may perform better than evidenced by the W3C DNT Working Group.