2016

When the Default Is No Penalty: Negotiating Privacy at the NTIA

Margot E. Kaminski
University of Colorado Law School

WHEN THE DEFAULT IS NO PENALTY: NEGOTIATING PRIVACY AT THE NTIA

MARGOT E. KAMINSKI†

ABSTRACT

Consumer privacy protection is largely within the purview of the Federal Trade Commission. In recent years, however, the National Telecommunications and Information Administration (NTIA) at the Department of Commerce has hosted multistakeholder negotiations on consumer privacy issues. The NTIA process has addressed mobile apps, facial recognition, and most recently, drones. It is meant to serve as a venue for industry self-regulation. Drawing on the literature on co-regulation and on penalty defaults, I suggest that the NTIA process struggles to successfully extract industry expertise and participation against a dearth of federal data privacy law and enforcement. This problem is most exacerbated in precisely the areas the NTIA currently addresses: consumer privacy protection around new technologies and practices. In fact, industry may be more likely to see the NTIA process as itself penalty-producing and, thus, be disincentivized from meaningful participation or adoption.

TABLE OF CONTENTS

† Assistant Professor, The Ohio State University Michael E. Moritz College of Law. Thanks to Kristelia García and to Dennis Hirsch, whose work in disparate areas inspired the ideas in this piece.

INTRODUCTION

The United States famously does not have omnibus federal data privacy law.[1] Instead, existing federal privacy law regulates the market or technologies by sector. One law governs children's privacy;[2] another governs health privacy;[3] another governs the use of information about videos that you watch.[4] New technologies and practices—ranging from mobile phones apps to facial recognition to drones—create significant data privacy issues that federal privacy law does not explicitly cover. The federal government's current approach to data privacy concerns raised by these technologies is the under-examined multistakeholder process at the National Telecommunications and Information Administration (NTIA).[5]

The NTIA is not the federal agency that springs to mind when discussing consumer privacy. Most think of the Federal Trade Commission (FTC) as the consumer privacy agency because the FTC has used its Section 5 authority to govern both consumer privacy and data security.[6] Perhaps the NTIA's relative obscurity is due to the fact that while the Department of Commerce has long been involved in setting privacy policy, the NTIA's current efforts are relatively new. The NTIA has been involved in this particular multistakeholder process since only 2012.[7] Or perhaps this obscurity stems from the fact that the NTIA does not enforce these best practices; it serves as a neutral negotiating forum for private stakeholders to arrive at these "voluntary, enforceable" best practices.[8]

Whatever the reason, the lack of discussion of the NTIA multistakeholder process in the literature is a significant oversight. The NTIA multistakeholder process is a key component of the White House's tout-

---

1. Paul M. Schwartz, *The Value of Privacy Federalism*, *in* SOCIAL DIMENSIONS OF PRIVACY 324, 324–27 (Beate Roessler & Dorota Mokrosinska eds., 2015).

2. *See* Children's Online Privacy Protection Act (COPPA) of 1998, 15 U.S.C. §§ 6501–6506 (2012).

3. *See* Health Insurance Portability and Accountability Act (HIPAA) of 1996 § 1177, 42 U.S.C. § 1320d-6 (2012).

4. *See* Video Privacy Protection Act (VPPA) of 1988, 18 U.S.C. § 2710 (2012).

5. The NTIA multistakeholder process was mentioned in passing by Justin Brookman. Justin Brookman, *Protecting Privacy in an Era of Weakening Regulation*, 9 HARV. L. & POL'Y REV. 355, 363, 363 nn.49–50 (2015).

6. Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 598–606 (2014).

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

8. *Id.* (stating the NTIA's role in the process is "to provide a forum for discussion and consensus-building among stakeholders"); *see also Privacy Multistakeholder Meetings Regarding Facial Recognition Techonology: February–June 2014*, NAT'L TELECOMM. & INFO. ADMIN. (Dec. 3, 2013) [hereinafter *Facial Recognition Technology*], https://www.ntia.doc.gov/other-publication/2013/privacy-multistakeholder-meetings-regarding-facial-recognition-technology-feb.

ed approach to data privacy.[9] The success or failure of this process has significant implications for how we regulate data privacy going forward.

Moreover, what's happening at the NTIA has broader implications for discussions of delegating regulation to private actors or incorporating standards that private actors have devised. Good governance likely needs the industry and technological expertise that private actors possess. The story of the NTIA's multistakeholder process shows, however, that certain regulatory conditions may be necessary to get private actors to put that expertise towards governing themselves.

I begin by describing the current multistakeholder process at the NTIA and explaining its origins. I then ask the necessary question: Is the process actually working? Answering that largely in the negative, I bring together literature on co-regulation with literature on penalty defaults to suggest that while private expertise may be necessary for effective governance in this realm, private actors will not co-regulate in the desired way unless the government sets a regulatory default that is worse than enforcement of best practices. I close with some important lessons learned.

I. WHAT IS THE NTIA DOING IN CONSUMER PRIVACY REGULATION?

Because regulating data privacy entails regulating fast-developing technologies, many have suggested that private industry is best equipped to self-regulate.[10] The government faces an expertise problem: it inevitably cannot gather expertise fast enough to keep up with technological development.[11] The obvious concern, however, is that private industry

---

9. Administration Discussion Draft: Consumer Privacy Bill of Rights Act of 2015, H.R. 1053, 114th Cong. § 301 (2015) [hereinafter Consumer Privacy Bill of Rights Act of 2015 Draft], https://www.whitehouse.gov/sites/default/files/omb/legislative/letters/cpbr-act-of-2015-discussion-draft.pdf (listing the multistakeholder process as the first step the Secretary of Commerce may make when deciding if a certain code of conduct should be considered a safe harbor); *see also* WHITE HOUSE, CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY 23–27 (2012) [hereinafter PRIVACY BLUEPRINT OF 2012], https://www.whitehouse.gov/sites/default/files/privacy-final.pdf ("The Administration encourages [all] relevant groups to participate in multistakeholder processes to develop codes of conduct that implement [the general principles in the Consumer Privacy Bill of Rights Act of 2015]. . . . [The] NTIA will lead the Department of Commerce's convening of stakeholders.").

10. DEP'T OF COMMERCE INTERNET POLICY TASK FORCE, COMMERCIAL DATA PRIVACY AND INNOVATION IN THE INTERNET ECONOMY: A DYNAMIC POLICY FRAMEWORK 5 (2010), https://www.ntia.doc.gov/files/ntia/publications/iptf_privacy_greenpaper_12162010.pdf; *see also* David Thaw, *Enlightened Regulatory Capture*, 89 WASH. L. REV. 329, 370–77 (2014) (describing how the expertise of private industry actors in the area of regulating data privacy can be borrowed to assist government in its regulation of the same); Dennis D. Hirsch, *The Law and Policy of Online Privacy: Regulation, Self-Regulation, or Co-Regulation?*, 34 SEATTLE U. L. REV. 439, 457–59 (2011).

11. 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, 98–99 (2013) (footnote omitted) (explaining one reason the government adopted the multistakeholder process was its fear that "[s]low-moving, notice-and-comment rulemaking [would] not be able to keep up with rapidly changing technologies, business practices, and consumer expectations. Moreover, the regulators

will self-regulate with its own best interests in mind.[12] Thus the crucial question is: How do we spur private industry involvement in data privacy regulation without allowing it to capture the process at the expense of the general public?

The White House's recent answer to this question is the proposed Consumer Privacy Bill of Rights Act (the Act), based on an earlier blueprint announced in a 2012 policy document.[13] The Act would create backstop federal privacy legislation consisting of a Privacy Bill of Rights (Title I), enforceable by states' attorneys general and the FTC (Title II). Against this backstop, private stakeholders could negotiate their own industry-specific codes of conduct at the Department of Commerce (Title III).[14] Upon approval by the FTC, these negotiated codes of conduct would serve as a safe harbor from liability for violating the Act.[15]

The White House has touted this approach in a number of policy documents addressing Big Data.[16] The problem for the White House is that Congress has not enacted the Act—not even close. With criticisms from both privacy advocates and regulatory skeptics, the administration could not find Congressional sponsors for the bill.[17] In the meantime, the Executive Branch decided to attempt this approach alone.

Starting in 2012, the White House directed the NTIA, which is housed in the Department of Commerce, to begin convening meetings between privacy stakeholders to negotiate sector-specific "legally enforceable" codes of conduct.[18] The White House explained that the NTIA "has the necessary authority and expertise" to conduct these meetings, based on its past participation in "other areas of Internet policy."[19] While

---

themselves [would] not be able to learn enough about quickly evolving industries to design intelligent rules for them").

12. Hirsch, *supra* note 10, at 458–59; Thaw, *supra* note 10, at 331.

13. Consumer Privacy Bill of Rights Act of 2015 Draft, *supra* note 9, at 1 (originally proposed in Feb. 2012; Act proposed in Feb. 2015); *see also* PRIVACY BLUEPRINT OF 2012, *supra* note 9, at 1.

14. Consumer Privacy Bill of Rights Act of 2015 Draft, *supra* note 9, at 17; *see also* PRESIDENT'S COUNCIL OF ADVISORS ON SCI. & TECH., EXEC. OFFICE OF THE PRESIDENT, BIG DATA AND PRIVACY: A TECHNOLOGICAL PERSPECTIVE 38, 40–41 (2014) [hereinafter BIG DATA AND PRIVACY], https://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdf.

15. Consumer Privacy Bill of Rights Act of 2015 Draft, *supra* note 9, at 17.

16. *See* BIG DATA AND PRIVACY, *supra* note 14, at 40–41; WHITE HOUSE, BIG DATA: SEIZING OPPORTUNITIES, PRESERVING VALUES 8–9 (2015), https://www.whitehouse.gov/sites/default/files/docs/20150204_Big_Data_Seizing_Opportunities_Preserving_Values_Memo.pdf; PRIVACY BLUEPRINT OF 2012, *supra* note 9, at 6.

17. Alex Wilhelm, *White House Drops 'Consumer Privacy Bill of Rights Act' Draft*, TECHCRUNCH (Feb. 27, 2015), http://techcrunch.com/2015/02/27/white-house-drops-consumer-privacy-bill-of-rights-act-draft/.

18. *Mobile Application Transparency*, *supra* note 7.

19. PRIVACY BLUEPRINT OF 2012, *supra* note 9, at 26. As statutory authority, the White House states "[the] NTIA is designated by statute as the 'President's principal adviser on telecommunications policies pertaining to the Nation's economic and technological advancement . . . .'" *Id.* at 26 n.29 (quoting 47 U.S.C. § 902(b)(2)(D) (2012)).

the NTIA is no stranger to privacy questions—a 1995 report discusses telecommunications privacy issues, for example[20]—it has been delegated an increasingly active role in privacy policy in recent years. The Department of Commerce established the Internet Policy Task Force in 2010, coordinating efforts at the NTIA with policy efforts at other agencies such as the U.S. Patent and Trademark Office. One of the Task Force's initiatives is to address Internet privacy.[21] The NTIA's multistakeholder meetings fall under the domain of this Internet Policy Task Force. The White House's recent placement of privacy multistakeholder meetings at the NTIA involves the agency in consumer privacy policy.

The White House explained in its 2012 Privacy Blueprint that, ideally, companies would voluntarily adopt the privacy codes of conduct developed at the NTIA. Once adopted, the code would become enforceable by the FTC under Section 5 of the FTC Act, "just as a company is bound today to follow its privacy statements."[22] On its face, this policy sounds relatively nonthreatening to companies. They may negotiate codes of conduct at the NTIA if they feel like it, and they will be subject to FTC enforcement only if they choose to adopt a particular code of conduct. Thus the model of how the NTIA process will work is that it should produce voluntary codes of conduct, signed by industry actors, and enforceable by the FTC only against those who sign on.

Even within the Privacy Blueprint, however, the White House appears to suggest broader enforcement potential.[23] On the one hand, codes of conduct might operate as a de facto safe harbor from FTC enforcement. On the other hand, the FTC might look to codes of conduct to establish the industry standards undergirding a Section 5 enforcement action. In other words, stakeholders may fear engaging in the NTIA process because the resulting industry code of conduct could trigger, rather than prevent, FTC enforcement action.

---

20. U.S. DEP'T OF COMMERCE, PRIVACY AND THE NII: SAFEGUARDING TELECOMMUNICATIONS-RELATED PERSONAL INFORMATION (1995), https://www.ntia.doc.gov/legacy/ntiahome/privwhitepaper.html.

21. DEP'T OF COMMERCE INTERNET POLICY TASK FORCE, CYBERSECURITY, INNOVATION AND THE INTERNET ECONOMY iv (2011), http://www.nist.gov/itl/upload/Cybersecurity_Green-Paper_FinalVersion.pdf ("In April 2010, Commerce Secretary Gary Locke established a Department-wide Internet Policy Task Force to address key Internet policy challenges.").

22. PRIVACY BLUEPRINT OF 2012, *supra* note 9, at 27; *see also* Brookman, *supra* note 5, at 363 n.49 ("The FTC would have jurisdiction over such codes because a statement of adherence to a code would be a consumer representation; if a company ended up violating such a statement, that would constitute a deceptive business practice under the law."); Press Release, Fed. Trade Comm'n, FTC Settles with Twelve Companies Falsely Claiming to Comply with International Safe Harbor Privacy Framework (Jan. 21, 2014), https://www.ftc.gov/news-events/press-releases/2014/01/ftc-settles-twelve-companies-falsely-claiming-comply (discussing how the FTC has enforced voluntary industry codes in the past); FTC v. Google *2012 - Misrepresentation of Compliance with NAI Code a Key Element*, IT LAW GROUP (2014), http://www.itlawgroup.com/resources/articles/69-ftc-v-google-2012-misrepresentation-of-compliance-with-nai-code-a-key-element.

23. PRIVACY BLUEPRINT OF 2012, *supra* note 9, at 30 ("In any investigation or enforcement action related to the subject matter of one or more codes, the FTC should consider the company's adherence to the codes favorably.").

Is this fear that codes of conduct will be enforced as industry standards against non-signatories reasonable? The FTC's privacy orders have been described by leading scholars in the area as creating "codified . . . best practices."[24] These scholars in fact characterize the ideal version of the FTC's enforcement process as waiting for an industry standard to emerge and then codifying it through FTC privacy orders.[25] In enforcement actions, the FTC usually compares a particular company's conduct to actual "industry standards writ large."[26] For example, in recent litigation challenging the FTC's authority to regulate data security under Section 5's unfairness prong, the FTC explained that to determine what constitutes "reasonable" data security, companies may look to, among other things, actual industry best practices.[27] The FTC also issues best practices as guidance, but tends not to rely on its own best practices for enforcement purposes.[28]

The question then is whether NTIA codes of conduct will be treated more like the FTC's own guidance in the area—that is to say, not generally used for determining the industry standard for enforcement purposes—or treated more like actual industry standards, which are frequently referred to in enforcement actions. At least initially, the FTC would be unlikely to look to NTIA best practices alone to determine reasonableness. However, if the NTIA process works the way the White House envisions, it will result in standards widely adopted by industry leaders, which would consequently nudge or dictate the industry standards on which FTC enforcement relies. If the NTIA system works as the White House envisions—creating industry codes of conduct that are then actually adopted by the majority of players in an industry—it is hard to imagine the FTC will not eventually look to the codes for guidance as to the industry standard in a sector in determining which enforcement actions to pursue.

---

24. Solove & Hartzog, *supra* note 6, at 586. Solove and Hartzog acknowledge, however, that currently, privacy best practices are more amorphous than their cybersecurity equivalents. *Id.* at 657 ("With regard to privacy, what constitutes good practice is more in dispute, although there are certainly some practices about which consensus has developed.").

25. Woodrow Hartzog & Daniel J. Solove, *The Scope and Potential of FTC Data Protection*, 83 GEO. WASH. L. REV. 2230, 2265 (2015) ("The FTC can wait until a consensus around specific standards develops in the industry and then codify them as this happens.").

26. Solove & Hartzog, *supra* note 6, at 626–27 (quoting E-mail from David Vladeck, Dir., Bureau of Consumer Prot., to authors (Oct. 3, 2013, 1:12 PM) (on file with the Columbia Law Review)).

27. F.T.C. v. Wyndham Worldwide Corp., 10 F. Supp. 3d 602, 616–17 (D.N.J. 2014) (noting that Wyndham could look to "industry guidance sources that [Wyndham] . . . itself seems to measure its own data-security practices against").

28. *See* Solove & Hartzog, *supra* note 6, at 626–27 (citing E-mail from David Vladeck, Dir., Bureau of Consumer Prot., to authors (Oct. 3, 2013, 1:12 PM) (on file with the Columbia Law Review)).

II. IS THE NTIA MULTISTAKEHOLDER PROCESS WORKING?

The White House has directed the NTIA to convene multistakeholder discussions on consumer privacy in three sectors: mobile applications;[29] facial recognition technology;[30] and most recently, drones.[31] The NTIA has convened discussions in these areas, concluding the code of conduct for transparency in mobile applications in 2013.[32] Discussions of the facial recognition code stalled in June 2015, when consumer advocate groups walked out of the process in protest.[33] Discussions of drones concluded in 2016; this author participated in them.[34]

The important question, for purposes of evaluating both how the White House currently handles data privacy and the viability of any future version of the Consumer Privacy Bill of Rights Act, is whether the NTIA multistakeholder process is working. In three words: it is not.

The success of the efforts can be judged along several axes.[35] First, how wide is participation in the process? Does it bring in meaningful representation from both industry and public interest groups, as intended? Second, how successful are the efforts at reaching consensus? Does the final code reflect influence by diverse participants? And third: How widely is the code actually adopted? We have evidence on the third question only with respect to the NTIA's mobile app work, but there is initial evidence as to participation in the other two processes. As charted below, for all three questions, in all three sets of negotiations, the answers are not encouraging.

A. Mobile Apps

The NTIA's first efforts focused on driving transparency in the privacy practices of mobile applications. The central issue was how to meaningfully alert mobile phone users to what kinds of information mobile phone applications collected and shared. This conversation was

---

29. *See Mobile Application Transparency*, *supra* note 7.

30. *See Facial Recognition Technology*, *supra* note 8.

31. *See Multistakeholder Process: Unmanned Aircraft Systems*, NAT'L TELECOMM. & INFO. ADMIN. (June 21, 2016) [hereinafter *Unmanned Aircraft Systems*], https://www.ntia.doc.gov/other-publication/2015/multistakeholder-process-unmanned-aircraft-systems.

32. *Mobile Application Transparency*, *supra* note 7; Angelique Carson, *Did NTIA's Multi-Stakeholder Process Work? Depends on Whom You Ask*, IAAP: PRIVACY ADVISOR (Sep. 3, 2013), https://iapp.org/news/a/did-ntias-multi-stakeholder-process-work-depends-whom-you-ask/.

33. Natasha Singer, *Consumer Groups Back Out of Federal Talks on Face Recognition*, N.Y. TIMES: BITS (June 16, 2015, 12:10 AM), http://bits.blogs.nytimes.com/2015/06/16/consumer-groups-back-out-of-federal-talks-on-face-recognition/.

34. *Unmanned Aircraft Systems*, *supra* note 31.

35. Ira Rubinstein suggested a six-factor normative framework for evaluating the efficacy of co-regulation: efficiency, openness and transparency, completeness when compared to FIPPs, strategies to address free rider problems, oversight and enforcement, and use of second-generation design features. Ira S. Rubinstein, *Privacy and Regulatory Innovation: Moving Beyond Voluntary Codes*, 6 ISJLP 355, 380 (2011). My normative framework roughly maps on to a subset of these factors: openness and transparency (who are the actors?); completeness when compared to other codes of conduct; and free rider problems. *See id.*

largely about what constitutes meaningful notice in the smartphone space. Since U.S. privacy largely centers around the idea of notice and consent, figuring out how to apply that model to small, mobile, ubiquitous screens is a central policy question in data privacy law.[36]

The initial meeting resulted in relatively high participation and sixty separate proposals; over time, however, fewer participants were willing to remain involved.[37] The drafting ended in the summer of 2013.[38] A number of civil liberties organizations supported the draft, but the Center for Digital Democracy (CDD) abstained and called instead for broad consumer privacy legislation and FTC regulation.[39] The CDD explained that the stakeholder process relied too heavily on voluntary and thus inadequate revelations by industry members about their practices.[40]

In terms of substance, the NTIA code can be compared to the FTC's February 2013 recommended best practices for mobile app transparency.[41] The FTC recommends that apps should provide just-in-time disclosures and obtain affirmative express consent when (a) collecting sensitive information outside the platform's API, or (b) sharing sensitive data with third parties.[42] The NTIA code, by contrast, suggests use of a single "short form notice"—that is, a notice that is easy to read and understand—that is "readily available from the application," but crucially only "encourages but does not require presentation of [the] short form notice prior to installation or use of the application."[43]

These are significantly different notice mechanisms. One (the FTC's approach) actively alerts a user to the collection or sharing of sensitive information at the moment the information is collected or shared. The other (the code of conduct's approach) is potentially hidden within the application, and need not be actively shown to the user at all. To be fair, many mobile applications at the time of negotiations had no privacy policies; the NTIA's modest proposal of adoption of a short-form policy looks like an improvement in that context. The disparity between the NTIA's suggested form of notice and the FTC's guidance on the issue, however, suggests limits on the idea that the NTIA process will arrive at

---

36. *See* Ryan Calo, *Code, Nudge, or Notice?*, 99 IOWA L. REV. 773, 787–89 (2014).

37. Brookman, *supra* note 5, at 363–64.

38. *See Mobile Application Transparency*, *supra* note 7.

39. Jeff Chester, *CDD Urges FTC to Review Proposed NTIA Code of Conduct*, CTR. FOR DIGITAL DEMOCRACY (July 26, 2013), https://www.democraticmedia.org/cdd-urges-ftc-review-proposed-ntia-code-conduct; *see also* Carson, *supra* note 32.

40. Chester, *supra* note 39 ("The stakeholder process is intrinsically flawed. It principally relies on industry to provide accurate information on the practices they actually engage in.").

41. *See* FED. TRADE COMM'N, MOBILE PRIVACY DISCLOSURES i–iii, 12 (2013), https://www.ftc.gov/sites/default/files/documents/reports/mobile-privacy-disclosures-building-trust-through-transparency-federal-trade-commission-staff-report/130201mobileprivacyreport.pdf.

42. *Id.* at 23.

43. SHORT FORM NOTICE CODE OF CONDUCT TO PROMOTE TRANSPARENCY IN MOBILE APP PURCHASES 2, 5 (NAT'L TELECOMMS. & INFO. ADMIN., Redline Draft 2013), https://www.ntia.doc.gov/files/ntia/publications/july_25_code_draft.pdf.

"best" practices, versus constitute a race to the bottom. Clarity is also a concern. A study of the NTIA proposal conducted by researchers at Carnegie Mellon concluded that "the current set of NTIA categories does not appear to offer a high level of transparency for users."[44]

Perhaps the most damning observation about the mobile apps process is that it did not result in widespread industry adoption. Consumer Watchdog pointed out that, while twenty industry participants "supported" the code, only two "endorsed" it—meaning, only two industry participants were willing to publicly commit to putting the code into practice, thus making it clearly legally enforceable.[45] On the other side of the issue, industry representatives raised usability concerns, explaining that the data gathering practices discussed at the meetings were not representative of practices in real life.[46] According to one commentator, "by and large the principles have been ignored by industry."[47] The NTIA process thus faces a significant free rider problem: industry may profit from the goodwill associated with the process, without taking on the costs of actually implementing even the lenient code.[48]

B. Facial Recognition

Next, the NTIA convened stakeholder discussions on facial recognition technologies.[49] Facial recognition technologies come in many forms. They can involve analysis of existing social media imagery, or they can involve surveillance of individuals in real and unexpected physical spaces. In the second context, facial recognition technologies raise many of the same policy questions as the Internet of Things: companies can use the technologies on individuals without a user agreement, and even without notice to the individual.[50] The issues raised are complex and entail discussing whether our approach to data privacy online is appropriate for data privacy entwined with the real physical world.

The NTIA process around facial recognition stalled in the summer of 2015, when consumer protection groups walked out of the negotia-

---

44. REBECCA BALEBAKO, RICHARD SHAY & LORRIE FAITH CRANOR, IS YOUR INSEAM A BIOMETRIC? EVALUATING THE UNDERSTANDABILITY OF MOBILE PRIVACY NOTICE CATEGORIES 10 (2013), https://www.cylab.cmu.edu/files/pdfs/tech_reports/CMUCyLab13011.pdf.

45. John M. Simpson, *Effort to Craft Apps "Transparency Code" Shows Futility of Multi-Stakeholder Process*, CONSUMER WATCHDOG (July 25, 2013), http://www.consumerwatchdog.org/newsrelease/effort-craft-apps-%E2%80%9Ctransparency-code%E2%80%9D-shows-futility-multi-stakeholder-process.

46. Grant Gross, *A Federal Push for Mobile Privacy Has Failed, Critics Say*, PCWORLD (Aug. 29, 2013), http://www.pcworld.com/article/2047775/critic-ntias-mobile-privacy-push-has-failed.html.

47. Brookman, *supra* note 5, at 363.

48. Rubinstein, *supra* note 35, 379–80.

49. *Privacy Multistakeholder Process: Facial Recognition Technology*, NAT'L TELECOMM. & INFO. ADMIN. (June 11, 2015) [hereinafter NTIA, *Privacy*], https://www.ntia.doc.gov/other-publication/2015/privacy-multistakeholder-process-facial-recognition-technology.

50. *See* Meg Leta Jones, *Privacy Without Screens & the Internet of Other People's Things*, 51 IDAHO L. REV. 639, 647 (2015).

tions.[51] The groups explained in a letter that they chose to walk out of the process because companies refused to even engage with the idea of opt-in consent to facial recognition.[52] Opt-in consent has been the basis of state legislation, and consumer protection and privacy organizations raised serious objections to the fact that it was not on the table at the NTIA.[53] It is unclear from the NTIA website whether the process has continued beyond July 28, 2015.[54]

The latest discussion draft of the code, evidently proposed by the International Biometric Industry Association (IBIA), dates from July 22, 2015.[55] The draft focuses on transparency and data security, with transparency constituting a dual approach of (i) available privacy policies, and (ii) notice that the technology is being used.[56] The draft language is sparse, largely repeating the Fair Information Practice Principles (FIPPs), such as collection limitation, the purpose specification principle, the use limitation principle, etc.

What little specific information the draft proposes, however, shows the limitations that frustrated privacy advocates.[57] While the draft advocates notice, it explains that such notice will be highly context-dependent. The draft states that notice should depend on the type of personal data used, how that data will be stored and used, and reasonable expectations of use of that data.[58] In other words, companies may at their own discretion, using vague factors, determine whether and when individuals might even receive notice of the use of individually-identifying facial recognition technologies.

The similarly sparse draft of NTIA's stakeholder guidelines also relies on notice and transparency.[59] The guidelines explain that entities using facial recognition technologies should "make available to subjects" their policies regarding biometric collection and use.[60] They explain that

---

51. Singer, *supra* note 33.

52. Andrea Peterson, *The Government's Plan to Regulate Facial Recognition Tech Is Falling Apart*, WASH. POST: SWITCH (June 16, 2015), https://www.washingtonpost.com/news/the-switch/wp/2015/06/16/the-governments-plan-to-regulate-facial-recognition-tech-is-falling-apart/.

53. *See id.* (citing Illinois and Texas as examples).

54. NTIA, *Privacy*, *supra* note 49 (announcing the most recent meeting as occurring July 28, 2015).

55. NAT'L TELECOMMS. & INFO. ADMIN., PRIVACY BEST PRACTICE RECOMMENDATIONS FOR COMMERCIAL BIOMETRIC USE (2014) [hereinafter NTIA, PRIVACY BEST PRACTICE], https://www.ntia.doc.gov/files/ntia/publications/ibia_ntia_7-22-15_discussion_draft.pdf.

56. *Id.* at 2.

57. *See* Alvaro M. Bedoya, *Why I Walked Out of Facial Recognition Negotiations*, SLATE (June 30, 2015, 11:56 AM), http://www.slate.com/articles/technology/future_tense/2015/06/facial_recognition_privacy_talks_why_i_walked_out.html;%20https://cdt.org/blog/cdt-withdraws-from-the-ntia-facial-recognition-process/.

58. *Id.* at 2; NTIA, PRIVACY BEST PRACTICE, *supra* note 55, at 2.

59. GUIDELINES FOR THE COLLECTION AND USE OF FACIAL RECOGNITION § 3 (NAT'L TELECOMMS. & INFO. ADMIN., Stakeholder Draft 2015).

60. *Id.*

notice should be given before the technology is employed, or alternatively may be given after employment if the subject can control use of the data.[61] Like the discussion draft, the stakeholder guidelines rely ies on a number of the FIPPs; and like the discussion draft, they nowhere contemplate that subjects might justifiably opt out of facial recognition—or be given the option to opt in, to begin with.

The FTC, by contrast, in October 2012 recommended best practices for facial recognition technologies that included an opt-out mechanism, and even more stringent opt-in consent in some cases.[62] The FTC described a "sliding scale approach to notice and choice," including choice mechanisms such as an ability to "walk away."[63] The FTC also contemplated more active choice mechanisms, such as "requir[ing] consumer interaction prior to processing the consumer's image."[64] As a second point of reference, the EU Article 29 Working Group report on facial recognition from March 2012 explicitly requires opt-in, requiring "valid consent . . . prior to acquisition" and notice constituting "sufficient information relating to when a camera is operating for the purpose of facial recognition."[65]

This is not to suggest that the NTIA process must or even should arrive at best practices in compliance with EU standards, or even identical to FTC recommendations. The process of producing NTIA codes of conduct is different, and perhaps the goal is different as well. But it is notable that both with respect to mobile applications and with respect to facial recognition, the NTIA's process arrived at notably lower standards of consumer privacy protection than those recommended by the FTC. Again, even those standards face a free rider problem: nobody appears to have adopted them as a working code.

C. Drones

In February 2015, the President instructed the NTIA to convene discussions about privacy and drones.[66] In May 2016, the NTIA announced the completion of the process.[67]

---

61. *Id.*

62. FED. TRADE COMM'N, FACING FACTS: BEST PRACTICES FOR COMMON USES OF FACIAL RECOGNITION TECHNOLOGY (2012), https://www.ftc.gov/sites/default/files/documents/reports/facing-facts-best-practices-common-uses-facial-recognition-technologies/121022facialtechrpt.pdf.

63. *Id.*

64. *Id.*

65. *Article 29 Data Protection Working Party Opinion 02/2012 on Facial Recognition in Online and Mobile Services*, at 7 (Mar. 22, 2012), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp192_en.pdf.

66. *See* Presidential Memorandum: Promoting Economic Competitiveness While Safeguarding Privacy, Civil Rights, and Civil Liberties in Domestic Use of Unmanned Aircraft Systems, WHITE HOUSE: OFFICE OF THE PRESS SECRETARY (Feb. 15, 2015), https://www.whitehouse.gov/the-press-office/2015/02/15/presidential-memorandum-promoting-economic-competitiveness-while-safegua.

Drones, or unmanned aircraft systems (UAS), pose similar but not identical privacy concerns to facial recognition technologies. Again, drones involve the surveillance of nonconsenting and often unknowing individuals in physical spaces. Unlike facial recognition, however, drones also enable surveillance from new and unexpected vantage points, reducing the efficacy of physical barriers.[68]

Participation by civil society in the NTIA drone process was markedly lower than the original level of participation in facial recognition discussions. Many of the civil liberties groups that participated in and withdrew from facial recognition discussions were largely absent from the discussions on drones, including the American Civil Liberties Union (ACLU), the Electronic Frontier Foundation (EFF), and CDD.[69] After the best practices were completed and released in May 2016, the ACLU, EFF, and Access Now released a letter criticizing the substance of the final agreement, noting that the document does not represent "best practices."[70] The Center for Democracy and Technology (CDT), by contrast, issued a statement of support for the process and results.[71]

Conversations during the process were derailed on several occasions with discussions of whether it was fair for the NTIA to single out drones for technology-specific regulation—a valid policy point that was nonetheless moot in light of the President's express Memorandum to the NTIA to focus on drones. One group of stakeholders took it upon themselves to come up with a document listing the positive social benefits of drones.[72] Another meeting devoted significant time to discussing First Amendment concerns with regulating drone newsgatherers and videographers.[73] These concerns are legitimate, but were perhaps overstated in

---

67. NAT'L TELECOMMS. & INFO. ADMIN., VOLUNTARY BEST PRACTICES FOR UAS PRIVACY, TRANSPARENCY, AND ACCOUNTABILITY § 2(a) [hereinafter FINAL BEST PRACTICES], https://www.ntia.doc.gov/files/ntia/publications/voluntary_best_practices_for_uas_privacy_transparency_and_accountability_0.pdf; *see also* Natasha Lomas, *US Agency Issues Privacy Guidance for Drone Operators*, TECHCRUNCH (May 20, 2016), https://techcrunch.com/2016/05/20/privacy-guidance-for-drone-operators-issued-by-us-agency/.

68. *See* Margot E. Kaminski, *Regulating Real-World Surveillance*, 90 WASH. L. REV. 1113, 1148 (2015).

69. *See* Peterson, *supra* note 52.

70. Letter from Access Now et al., to John Morris, Assoc. Adm'r & Dir. of Internet Policy, Nat'l Telecomms. & Info. Admin. (May 24, 2016) [hereinafter Access Now Letter], https://www.ntia.doc.gov/files/ntia/publications/aclu_access_now_eff_5-23_letter_on_uas_best_practices.pdf.

71. *Privacy and Civil Liberties Protection at Heart of NTIA Best Practices for Drones*, CTR. FOR DEMOCRACY & TECH. (May 18, 2016) [hereinafter *Privacy and Civil Liberties Protection*], https://cdt.org/press/privacy-and-civil-liberties-protections-at-heart-of-ntia-best-practices-for-drones/.

72. *NTIA Working Grp. on UAS: Positive Societal Benefits* 1–8 (Nov. 19, 2015) (Nat'l Telecomm. & Info. Admin., Working Draft), https://www.ntia.doc.gov/files/ntia/publications/2015-11-19_compilation_of_positive_societal_benefits_-_ntia_working_grou.pdf.

73. Letter from Charles D. Tobin, Partner, Holland & Knight LLP, to Nat'l Telecomms. & Info. Admin. (Nov. 18, 2015), https://www.ntia.doc.gov/files/ntia/publications/ntia_best_practices_-_11.17.2015_news_media_coalition.pdf.

the context of attempts to develop voluntary industry privacy best practices rather than direct government regulation.

The group worked off of a Combined Draft[74] containing elements from an earlier draft proposed by civil liberties organization, the Center for Democracy & Technology (CDT),[75] and elements from an earlier draft proposed by the law firm Hogan Lovells.[76] The two proposals converged on the basic structure of the issues, including provisions on notice, collection, sharing, and data security policies. Both agreed, for example, that best practices involve informing others about the use of drones to gather data.[77] Both agreed, as well, that best practices for commercial drone use should entail avoiding the use of drones "for the specific purpose of persistent and continuous collection of personal or private data about specific individuals."[78]

The two proposals differed significantly, however, on important details. Some of the most marked differences between the two proposals are as follows. One major difference concerned using drones to gather data without consent. The CDT proposal suggested that in the absence of a compelling need or informed consent, commercial UAS operators should avoid using UAS "for the specific purpose of intentionally collecting personal data . . . [w]here the operator knows the data subject has a reasonable expectation of privacy."[79] The Hogan Lovells proposal, while suggesting that companies should as a general matter aim to minimize data collection,[80] allowed drones to be used to purposefully collect personal data without consent.[81] The final version adopted the CDT language, but the final language includes a loophole for drone operators to collect personal data without consent if they can demonstrate a "compelling need" to do so.[82]

Instead of addressing the gathering of information, the Hogan Lovells proposal largely targeted misuse of the data collected. The draft stated that personal data gathered without consent or not pursuant to a contract should not be used "in an adverse manner" for employment,

74. *See* CTR. FOR DEMOCRACY & TECH., UAS PRIVACY BEST PRACTICES (2015), https://www.ntia.doc.gov/files/ntia/publications/cdt_uas_best_practices_draft_v2_111615_clean.pdf.

75. *See id.* at 1.

76. *See* HOGAN LOVELLS, PRIVACY, TRANSPARENCY, AND ACCOUNTABILITY—VOLUNTARY BEST PRACTICES FOR COMMERCIAL AND PRIVATE USE OF UNMANNED AIRCRAFT SYSTEMS (2015), https://www.ntia.doc.gov/files/ntia/publications/bestpracticesdraft11_19_hogan_lovells.pdf.

77. *Id.* at 4; CTR. FOR DEMOCRACY & TECH, *supra* note 74, at 4.

78. CTR. FOR DEMOCRACY & TECH, *supra* note 74, at 6; HOGAN LOVELLS, *supra* note 76, at 4.

79. CTR. FOR DEMOCRACY & TECH., *supra* note 76, at 6.

80. HOGAN LOVELLS & CTR. FOR DEMOCRACY & TECH., VOLUNTARY BEST PRACTICES FOR COMMERCIAL AND PRIVATE USE OF UNMANNED AIRCRAFT SYSTEMS: PRIVACY, TRANSPARENCY, AND ACCOUNTABILITY 2 (2015) [hereinafter BEST PRACTICES COMBINED DRAFT], https://www.ntia.doc.gov/files/ntia/publications/combined_draft_working_group_12_22_2015.pdf.

81. *Id.* at 7 (noting that unlike the CDT proposal, the Hogan Lovell's proposal contains no consent requirement).

82. FINAL BEST PRACTICES, *supra* note 67, at 4.

credit, or health care-related decisions.[83] The Hogan Lovells draft envisioned permitting other commercial uses of the data.[84] The final version of the best practices, while adopting more restrictions on gathering information than envisioned in the Hogan Lovells draft, mirrors the Hogan Lovells draft in listing only several specific prohibited information uses, such as determining employment eligibility or credit eligibility.[85]

A third significant difference involved the treatment of the airspace above private property. The CDT proposal was adamant on this issue, suggesting that UAS operators should make a reasonable effort (a) not to enter private property or airspace without informed prior consent, and (b) to minimize operations even in public airspace over private property without informed prior consent.[86] The Hogan Lovells draft took a different approach. It suggested that drone operators should make a reasonable effort to prevent drones that collect personal data from entering public airspace over private property "if the UAS operation will substantially interfere with the use and enjoyment of the property."[87] This, it should be noted, effectively just restates state nuisance law. The final version of the best practices suggests that drone operators should make a reasonable effort to minimize operations over or within private property without consent or legal authority, but creates a significant loophole where such flight impedes the purpose for which the UAS is used (which could be anything) or conflicts with FAA guidelines.[88]

A fourth significant difference involves the use of drone-gathered information for targeted marketing. While the Hogan Lovells proposal suggested that Commercial UAS operators should avoid using or sharing personal data for use in targeted marketing, they restrict that suggestion to situations "[w]here the operator has actual knowledge that the data subject has an expectation of privacy."[89] In other words, when a drone operator lacks actual knowledge of an expectation of privacy, it can use personal data for use in targeted marketing. By contrast, the CDT version suggested that UAS operators should make a reasonable effort to avoid using or sharing personal data for marketing purposes, unless it has been obfuscated or deidentified, or the data subject provides informed prior consent to disclosure.[90] The Hogan Lovells system envisioned a default of allowing use of drone surveillance as an input for individually targeted marketing; the CDT version envisioned a default of disallowing it, unless the data subject consents or has been deidentified.

---

83. HOGAN LOVELLS, *supra* note 76, at 7–8.
84. *Id.* at 9.
85. FINAL BEST PRACTICES, *supra* note 67, at 5.
86. BEST PRACTICES COMBINED DRAFT, *supra* note 80, at 8.
87. *Id.*
88. FINAL BEST PRACTICES, *supra* note 67, at 3.
89. BEST PRACTICES COMBINED DRAFT, *supra* note 80, at 10.
90. *Id.*

The final best practices document echoes the CDT proposal, directing drone operators to make a reasonable effort to avoid sharing personal data for marketing purposes without consent.[91] However, the best practices expressly contemplate using drone-gathered data for marketing in the aggregate. This leaves significant incentives in place for gathering information about individuals, even if that information will later be reduced to statistical information.[92]

A fifth significant difference between the CDT and Hogan Lovells proposals concerned the extent to which the subject of drone surveillance can access, correct, or delete the gathered data. The Hogan Lovells proposal suggested allowing data subjects "reasonable means to review" gathered data, and that UAS operators should take reasonable measures to maintain data accuracy.[93] It did not, however, provide any mechanism for individuals to request the deletion of data. The CDT proposal suggested that if an individual requests that a UAS operator "correct, destroy, obfuscate, or deidentify personal data about the individual," in the absence of need for that data to "fulfill a purpose for which the UAS is used," the UAS operator should honor this request.[94] The final version suggests only that UAS operators establish a process for receiving requests to delete data, without committing to actual deletion.[95]

During the process, CDT drafted a document detailing the many additional differences between the drafts.[96] Largely, the differences boiled down to the difference between envisioning drone use as just another extension of online surveillance practices, versus distinguishing drone use as different because it involves gathering information about nonconsenting individuals in a wide variety of physical locations.

In May 2016, the process was finalized, and the NTIA released a final version of the best practices.[97] CDT pointed out the positives, noting that the best practices restrict continuous collection of data about individuals, require drone operators to minimize both operations and surveillance over private property, and encourage drone operators not to share information for marketing purposes without consent.[98] The ACLU, EFF, and Access Now, by contrast, presented a strikingly different view. These organizations critiqued the document for allowing drone operators to collect private data without consent; allowing persistent, continuous sur-

91. FINAL BEST PRACTICES, *supra* note 67, at 5.
92. BEST PRACTICES COMBINED DRAFT, *supra* note 80, at 10.
93. *Id.*
94. *Id.*
95. FINAL BEST PRACTICES, *supra* note 67, at 8.
96. Memorandum from Harley Geiger, Ctr. for Democracy & Tech., to NTIA Unmanned Aircraft Sys. Privacy Working Grp. (Nov. 22, 2015), https://www.ntia.doc.gov/files/ntia/publications/comparison_of_cdt_hogan_draft_best_practices_for_drone_privacy.pdf.
97. *See* FINAL BEST PRACTICES, *supra* note 67.
98. *Privacy and Civil Liberties Protection*, *supra* note 71.

veillance without consent, even in traditionally private spaces; and allowing the use of the data for certain purposes without consent.[99]

The vastly differing readings of the document largely stem from how skeptically one views the various and numerous potential loopholes contained within it. If companies wish, they can read these loopholes (such as exceptions for "compelling purposes," or requirements of just "reasonable efforts") to largely obviate the good parts of these best practices. The proof will be in execution and adoption.

In April 2016, the Senate passed a version of FAA reauthorization that would preempt state drone laws, including drone-specific privacy laws, and would instruct Congress to build on the NTIA best practices and recommendations in crafting federal legislation.[100] The reactions of the various civil liberties organizations discussed above, in conjunction with the more general flaws of the process outlined here, suggest that over-reliance on the NTIA's output to frame federal drone privacy policy in the place of state laws would be ill-advised.

III. PLACING THE PROCESS IN THE LITERATURE: CO-REGULATION AND PENALTY DEFAULTS

Given how laborious the NTIA process is, why is this administration engaging in it? The NTIA process is founded on the idea that, especially with regards to evolving technologies, industry is best informed and best equipped to determine the best way to regulate itself. The government must figure out a way to involve industry in its own regulation; otherwise, governance risks significant missteps due to lack of knowledge, or overburdening particular technologies due to lack of expertise. In this section, I discuss some of the relevant academic literature that encourages incorporating private expertise into governance, especially in the data governance space.[101]

If it is a good idea to involve industry in regulation, then why has this particular method of involvement been relatively unsuccessful? NTIA negotiations have set weak standards that industry largely has not adopted, and face dwindling participation by groups on all sides. While there are multiple potential criticisms of the NTIA process,[102] the prob-

99. Access Now Letter, *supra* note 70.

100. Federal Aviation Administration Reauthorization Act of 2016, S. 2658, 114th Cong. §§ 2104, 2142 (2016), https://www.congress.gov/bill/114th-congress/senate-bill/2658; *see also* Malanie Zanona, *Senate Send FAA Reauthorization to House*, HILL (April 19, 2016, 12:46 PM), http://thehill.com/policy/transportation/276828-senate-sends-faa-reauthorization-to-house.

101. *See generally* Hirsch, *supra* note 11; Hirsch, *supra* note 10; Rubinstein, *supra* note 35; Thaw, *supra* note 10.

102. For example, the NTIA subject matter has been technology- or at least sector-specific. This irritates industry, which feel targeted in the absence of general data privacy law. Another possible criticism asks whether the NTIA is the right agency for this process. The DOC has a mission to encourage economic growth. Critics have noted that this mission runs in conflict with consumer protection, in this space. *See* Chester, *supra* note 39.

lem largely reduces to the current structure of our federal data privacy regime.

In the second part of this section, I briefly discuss the literature on "penalty defaults" to provide needed context for the NTIA's struggles. The idea of a penalty default is that the government can set a baseline that spurs private parties to negotiate towards a better outcome.[103] Scholars largely employ this concept to discuss the regulatory backdrop necessary to encourage more efficient private ordering.[104] I propose that the concept of penalty defaults, primarily used to discuss private contracting, can be useful for discussions of co-regulation like that encountered here. In the absence of a worse regulatory alternative—that is, enforceable federal data privacy law—industry has little incentive to meaningfully participate in the NTIA process.

A. Co-Regulation: Drawing on Industry Expertise

The White House has explained that its primary motive in involving industry in the privacy space is to harness industry expertise in fast-moving technological areas.[105] The academic literature addressing co-regulation, also known as collaborative governance, describes the potential benefits of this approach.[106] Potential benefits of co-regulation include obtaining unique knowledge and expertise from industry members; arriving at more realistic and cost-effective, workable, and innovative results; creating a stronger sense of industry ownership over rules and thus higher compliance; and creating more politically practicable and lower-cost processes.[107]

While I by no means attempt here to cover the vast literature on collaborative governance, the work of three scholars writing about co-regulation in the data governance space is particularly relevant to discussions of the NTIA. Dennis Hirsch, responding to early versions of the White House's safe harbor proposal, has studied co-regulation of data protection in the Netherlands, where industry actors collaborate with the Dutch government to set sector-specific codes.[108] Hirsch noted both

---

103. Ian Ayres & Robert Gertner, *Filling Gaps in Incomplete Contracts: An Economic Theory of Default Rules*, 99 YALE L.J. 87, 91 (1989).

104. *See, e.g.*, Kristelia A. García, *Penalty Default Licenses: A Case for Uncertainty*, 89 N.Y.U. L. REV. 1117, 1122 (2014) (identifying "penalty default licenses" and penalty defaults in general as a mechanism for inducing private ordering).

105. *See* Hirsch, *supra* note 10, at 466–68.

106. *See* Hirsch, *supra* note 11, at 88 ("[P]roponents of collaborative governance claim that it can combine the flexibility of business savvy of industry self-regulation with the accountability and public-spiritedness of government rules . . . ."); *see also* Hirsch, *supra* note 10, at 441 (noting that co-regulation can provide the "flexibility of self-regulation while adding the supervision and rigor of government rules"); Thaw, *supra* note 10, at 333 (noting the possibility to "increase both the representative legitimacy and the efficacy of the regulatory process").

107. Hirsch, *supra* note 10, at 466–67 (citing Jody Freeman, *Collaborative Governance in the Administrative State*, 45 UCLA L. REV. 1, 26 (1997)); *see also* Rubinstein, *supra* note 35, at 379–80.

108. Hirsch, *supra* note 11, at 120–23.

strengths and weaknesses in the system.[109] The strengths largely involved obtaining information from industry that regulators otherwise would not have accessed, and building productive relationships between industry and regulators founded on mutual trust.[110] I discuss the weaknesses further below.

David Thaw, writing about the creation of the Health Insurance Portability and Accountability Act (HIPAA) Security Rule, similarly touted the benefits of involving nongovernmental expertise in the setting of cybersecurity standards, through an informal version of negotiated rulemaking, also known as "reg neg" or "neg reg."[111] Thaw explained that in the context of the HIPAA Security Rule, a committee of nongovernmental individuals came up with a rule that departed from its members' individual interests and in fact served the public good.[112] Industry buy-in to the rule was high, as a consequence of the collaborative process.[113]

Ira Rubinstein, writing more generally about the potential role of co-regulation in U.S. privacy law, highlighted three examples of various kinds of existing privacy co-regulation: (1) the Network Advertising Initiative (NAI); (2) the U.S.-E.U. Safe Harbor Agreement; and (3) the Children's Online Privacy Protection Act (COPPA) Safe Harbor.[114] Rubinstein concluded that the COPPA Safe Harbor process produced the best co-regulatory efforts of the three, covering substantive privacy requirements while facing minimal free rider problems and invoking meaningful government enforcement by the FTC.[115] He noted, nonetheless, that the COPPA process itself was not particularly successful, pointing to too-strict statutory requirements as creating inadequate incentives for industry to self-regulate.[116]

Co-regulation is not a panacea; there are clear potential downsides. Potential costs include gaming of the system by industry using its informational advantage to obtain weaker rules; a reduction in the public's opportunity to participate; capture; lack of enforcement; and deterring new entrants through coordination by established firms.[117] Many of the checks on co-regulation involve attempted checks on regulatory capture.[118] The failures of the NTIA process, however, are not a matter of

109. *Id.* at 151–55.
110. *Id.* at 154.
111. Thaw, *supra* note 10, at 353–55.
112. *Id.* at 364–65.
113. *Id.* at 363.
114. Rubinstein, *supra* note 35, at 384, 390, 394.
115. *Id.* at 397–98.
116. *Id.* at 398–99.
117. Hirsch, *supra* note 10, at 468 (citing NEIL GUNNINGHAM & DARREN SINCLAIR, LEADERS AND LAGGARDS: NEXT-GENERATION ENVIRONMENTAL REGULATION 104–05 (2002)).
118. Hirsch, *supra* note 11, at 152 (suggesting third party audits to increase compliance); *id.* at 153 (suggesting opening up the process to include additional stakeholders such as consumer or

capture, or at least not in the traditional sense that a particular industry controls the outcome of the process. The process is open and collaborative, and the NTIA itself serves as a neutral convener rather than a vocal party. Something else has gone awry. To understand what, I turn to a second body of relevant literature: on penalty defaults.

B. Penalty Defaults: Getting Private Actors to the Table

The literature on penalty defaults arises in the context of contract law.[119] Penalty defaults are regulations that spur private parties to contract by setting a default that neither party wants.[120] Penalty defaults should be used, the reasoning goes, to prompt information exchange between private parties and encourage private ordering that is more efficient than what the government could devise.[121] Thus the rationale for penalty defaults is similar to the rationale for collaborative governance: private parties are often better situated with respect to expertise and knowledge about an area than the government. Both literatures address attempts to draw private parties into the process of creating more efficient arrangements.

Some discussion of regulatory defaults focuses on trying to set the best default, based on the behavioral understanding that most people will not opt out.[122] But discussion of penalty defaults focuses instead on welfare maximizing by setting an undesirable default, thus encouraging information flow and negotiations between private actors.[123] Prospect theory posits that people make decisions based on potential gains and losses.[124] Setting a negative default thus pushes even risk-averse players to engage in negotiations.

The literature on co-regulation or collaborative governance engages, albeit not explicitly, with the idea of the necessity of penalty defaults. Hirsch, Thaw, and Rubinstein all identify conditions necessary for privacy co-regulation to succeed. Similarly, Philip Harter, the source of nego-

---

privacy advocacy groups, but recognizing that this may stall negotiations). Thaw refers to his approach as "enlightened regulatory capture," but his requirements nonetheless target capture concerns. Thaw, *supra* note 10, at 358–59, 371 (discussing FACA openness requirements and the requirement that process include reduced-bias subject matter experts who are not subject to influence as a function of their employment).

119. Ian Ayres, *Regulating Opt-Out: An Economic Theory of Altering Rules*, 121 YALE L.J. 2032, 2044 (2012) (advocating using rules "to encourage contracting parties to choose the default or non-default options that they jointly prefer").

120. Ayres & Gertner, *supra* note 103, at 91.

121. *Id.*

122. Cass R. Sunstein & Richard H. Thaler, *Libertarian Paternalism Is Not an Oxymoron*, 70 U. CHI. L. REV. 1159, 1161 (2003) ("What [people] choose is strongly influenced by details of the context in which they make their choice, for example default rules.").

123. *See* García, *supra* note 104, at 1131 ("This view focuses on selecting an unpalatable default. . . . [C]ontracting entities [may] be encouraged to negotiate more efficient deal terms to avoid an unpalatable default.").

124. Daniel Kahneman & Amos Tversky, *Prospect Theory: An Analysis of Decision Under Risk*, 47 ECONOMETRICA 263, 263 (1979).

tiated rulemaking, listed the conditions necessary for that process to succeed. Looking to these conditions in conjunction with an understanding of penalty defaults explains why the NTIA process is not working as the White House desires.

One of Hirsch's recommendations to the United States, derived from observation of the Dutch system, is to pass a baseline privacy statute. The United States should pass the statute "not only for the privacy protections it will bring, but also to provide a structure for the industry codes and to give companies a strong incentive to come to the table and negotiate a code of conduct."[125] Hirsch noted that one of the Dutch industries' main motivations for drafting codes of conduct "was that it allowed them to clarify the Data Protection Act and achieve a degree of regulatory certainty."[126] In other words, the Dutch Data Protection Act served as a penalty default, creating bounded uncertainty that drove industry to the negotiating table.

Thaw similarly notes that during the HIPAA Security Rule negotiations, the relevant committee believed "that if they failed to act, other regulators or legislators would, and that would be a suboptimal outcome."[127] He lists this as one of his five characteristics of "enlightened regulatory capture:" a perceived detriment to industry if the process fails.[128] Participants in co-regulation must believe, in other words, that there will be negative and likely-to-occur consequences if they fail.[129] They must believe that there is a penalty default. Thaw points out that negative consequences are the other side of the coin of one of Harter's requirement for negotiated rulemaking: an opportunity for parties to gain.[130]

Rubinstein calls for careful consideration of industry incentives in creating baseline privacy legislation.[131] That legislation should include both carrots and sticks, such as a tiered liability system or a threat of stricter regulations.[132] In fact, Rubinstein observes that "the covenanting approach in the U.S. arises only when there is a credible threat of federal privacy regulation and firms sit down with regulators to negotiate a code of conduct in lieu of regulation."[133] Self-regulation works best when industry faces potential or actual negative consequences in the alternative.

---

125. Hirsch, *supra* note 11, at 159.
126. *Id.*
127. Thaw, *supra* note 8, at 365.
128. *Id.* at 371.
129. *Id.* at 372.
130. *Id.* at 371; Philip J. Harter, *Negotiating Regulations: A Cure for Malaise*, 71 GEO. L.J. 1, 43 (1982).
131. Rubinstein, *supra* note 35, at 415.
132. *Id.* at 416.
133. *Id.* at 401.

Industry actors may gain from co-regulation in a variety of ways. The gains may be reputational or emotional. In Thaw's example, industry actors considered service on the relevant committee to be a professional honor.[134] In the context of newer, developing technologies, however, the "gain" will largely constitute avoiding a worse default. In the absence of that default, industry actors are unlikely to buy in to the process of negotiating codes of conduct.

IV. LESSONS FOR U.S. DATA PRIVACY LAW

The core concept of penalty defaults is fairly intuitive: people will negotiate around settings they don't like. For productive co-regulation to occur, the costs of the default must be higher than the costs of participating in co-regulation.[135] This is a fairly intuitive observation, and one clearly applicable to the failure of the NTIA's multistakeholder process.

The penalty default literature has given thought to the pros and cons of different kinds of undesirable default settings. One idea might be to set a punitive default that clearly favors one party over the other.[136] This approach, however, risks entrenching negotiating power in the favored party.[137] In the context of data privacy, this could occur in two ways: by setting a punitive default heavily penalizing privacy violations, or by setting a default of not penalizing privacy violations (close to the current situation) thereby "punishing" those whose privacy is violated. Under the former, privacy advocates and consumer groups would have little incentive to negotiate alternative regimes. Under the latter, which is roughly descriptive of current U.S. law, industry would have little incentive to negotiate. Thus under the current U.S. regime, industry's negotiating position is entrenched. But there are difficulties with setting federal penalties. Swinging the pendulum too far in the other direction will not drive co-regulation, and government decisions over setting the level of appropriate punishment face exactly the kinds of information problems that collaborative governance seeks to remedy.

Another way to establish a penalty default, however, is to use uncertainty to the government's advantage. This approach could be particularly useful in privacy governance, which is rife with many types of uncertainty. Technological innovation can perpetuate uncertainty.[138] Potential government intervention can introduce uncertainty.[139] The implementation of standards, such as those proposed in the Consumer Privacy Bill of

134. Thaw, *supra* note 10, at 359.

135. Rubinstein, *supra* note 35, at 373 (recognizing this assertion when discussing Coasean bargaining, but not explicitly identifying it as a penalty default).

136. Garcia, *supra* note 104, at 1163.

137. *Id.*

138. *Id.* at 1172.

139. *Id.*; *see also* Rubinstein, *supra* note 35, at 401 (discussing negotiations of privacy covenants at the GNI under uncertainty).

Rights Act, rather than specific rules, can introduce uncertainty as to government interpretation.[140]

Uncertainty influences decisionmaking.[141] The literature on penalty defaults suggests that the government can actively use uncertainty to nudge desirable decisionmaking. Regulators can use uncertainty, paradoxically, to *increase* efficiency by nudging risk-averse private actors into negotiations.[142] There are several important caveats to this claim. First, uncertainty must affect both parties—not necessarily equally, but disproportionate uncertainty will reduce efficiency again by entrenching the interests of one party.[143] Second, uncertainty cannot just be general uncertainty; it should be sufficiently bounded such that parties are motivated to negotiate.[144] Unbounded uncertainty often leads to inefficiency and under-compliance.[145] Bounded uncertainty—uncertainty of a relatively small amount and defined kind—leads to negotiations, especially when the uncertainty is likely to resolve into a penalty default.[146] Thaw's, Hirsch's, and Rubinstein's examples all support bounded uncertainty as an effective way of driving co-regulation in the privacy space.

What are the lessons for U.S. data privacy law? Coupled with evidence from the NTIA negotiations thus far, this suggests that both the current penalties and the current levels and kinds of uncertainty in the U.S. privacy regime are not enough to drive industry to the table in efficiency-maximizing ways. In other words, what penalties there are in U.S. privacy law are not high enough, or likely enough to be enforced against a particular industry actor, to drive participation by most of the industry actors with whom the government wants to co-regulate.

The NTIA process teaches that the current backdrop of potential FTC enforcement is not enough to get industry to the table. Moreover, the possibility of FTC enforcement of the codes of conduct themselves

140. García, *supra* note 104, at 1173 (citing Louis Kaplow, *Rules Versus Standards: An Economic Analysis*, 42 DUKE L.J. 557, 605 (1992)).

141. *See, e.g.*, Christine Jolls, Cass R. Sunstein & Richard Thaler, *A Behavioral Approach to Law and Economics*, 50 STAN. L. REV. 1471, 1518–19 (1998); Amos Tversky & Daniel Kahneman, *Advances in Prospect Theory: Cumulative Representation of Uncertainty*, 5 J. RISK & UNCERTAINTY 297 (1992).

142. García, *supra* note 104, at 1169; *see also* Ian Ayres & Eric Talley, *Solomonic Bargaining: Dividing a Legal Entitlement to Facilitate Coasean Trade*, 104 YALE L.J. 1027, 1035 (1995) (showing "how ambiguity can induce bargainers to act more cooperatively").

143. García, *supra* note 104, at 1169; *see also* James Gibson, *Risk Aversion and Rights Accretion in Intellectual Property Law*, 116 YALE L.J. 882, 884 (2007) (explaining how uncertainty in copyright law combined with "risk aversion that pervades . . . copyright industries" results in unnecessary and thus inefficient licensing); Richard Craswell & John E. Calfee, *Deterrence and Uncertain Legal Standards*, 2 J.L. ECON. & ORG. 279, 280 (1986).

144. García, *supra* note 104, at 1132–33 (explaining that "bounded" uncertainty in the statutory license context in copyright includes knowing that the penalty default will at some point exist, and knowing the form in which it will eventually exist).

145. *Id.* at 1176.

146. *Id.* at 1177 (describing "the efficiency-enhancing effects of bounded uncertainty coupled with an unpalatable fallback").

actually drives industry to view both the negotiation and adoption of codes of conduct as leading to more likely enforcement by the FTC. The current system is precisely backwards: industry views the NTIA codes of conduct as potentially creating a penalty, not avoiding one. This increased possibility of FTC enforcement discourages industry from adopting codes of conduct once they have been created, exacerbating the free rider problem. And it discourages industry from even negotiating, out of fear that completed codes might be viewed as actual industry standards by the FTC, driving FTC enforcement even without explicit adoption of the codes by particular players.

The faults in the NTIA process further teach that the current state of unbounded uncertainty over whether Congress might enact federal data privacy law is not enough, by itself, to drive industry actors to the negotiating table.[147] The absence of data privacy legislation certainly leads to regulatory uncertainty. As John Morris, associate administrator and director of Internet policy at the NTIA, expressed: "We're trying to work on facial recognition without legislation . . . . Consumers and companies need to know what the rules are for this technology and we think stopping the discussion at this point doesn't get clarity that's needed."[148] But the failure of the NTIA process shows that the current lack of regulatory certainty is by itself not enough to drive effective information disclosure and negotiations.

The failure of the NTIA process, viewed through the lens of penalty default literature, suggests that a voluntary multistakeholder technique that has been shown to work in the technical standard space is not appropriate when applied to privacy.[149] Thaw argues, in the cybersecurity context, that there is nothing particularly special about technical standards, since the purpose of administrative law generally is to hone government expertise and harness private expertise.[150] He does suggest, however, that the linked nature of industry interests in the cybersecurity space—the fact that one player's failure will have negative externalities for other players—incentivizes players to come to the table to self-regulate.[151] The lens of penalty defaults suggests that in some technologically complex subject matter areas, a lack of coordination between actors may itself serve as a penalty default, preventing interoperability or leaving room for the types of negative externalities Thaw discusses. In data privacy negotiations, by contrast, the players tend not to come into the room seeking

147. *Contra id.* at 1180 (describing uncertainty over federal copyright lawmaking as driving private ordering in that space).

148. Peterson, *supra* note 52.

149. Thanks to Dennis Hirsch for this observation. Compare the NTIA stakeholder process to W3C.

150. Thaw, *supra* note 10, at 369 ("The idea that a highly technical subject would distinguish cybersecurity regulation from other regulation overlooks one of the core purposes of administrative agencies.").

151. *Id.* at 368.

consensus, and the subject matter of privacy, at least for now, produces no natural penalty for failure negotiate.[152]

To drive productive co-regulation in this space, the U.S. privacy regime must increase penalties, and-or shift from unbounded to bounded uncertainty. This could be accomplished through the enactment of something like the Consumer Privacy Bill of Rights Act, which describes data practices in broad standards, backed by FTC enforcement. The Act proposes creating, in other words, a penalty default with more bounded uncertainty over what, exactly, the standards require. For that system to work, however, FTC enforcement will have to occur at a high enough probability, and with high enough penalties, to drive actors to meaningfully negotiate more efficient alternatives.[153] The political will for this type of legislation does not appear high; perhaps, however, pressure from the EU over data privacy may spur Congress to more seriously consider it.[154]

Federal data privacy legislation that establishes a penalty default using bounded uncertainty is likely to be the best option for driving the kind of privacy co-regulation that our government envisions. As we wait for federal legislation, however, there may be other ways to presently improve the NTIA process. First, Congress could propose sector-specific legislation, creating the pending threat of regulation even if it does not intend to enact it, more obviously bounding the uncertainty under which the NTIA negotiations happen. Pending legislation has led to industry self-regulation in the past.[155] Second, the NTIA could play an information-gathering function in which it highlights for participants the other regulatory options on the table, including costly state-by-state regulation, and any Congressional proposals.

Third, the FTC could more visibly play the hammer, or the penalty default, targeting precisely those industries in which the NTIA wants to drive negotiations, to provide an unpalatable backstop. The FTC could either enforce in spaces where NTIA negotiations have failed, or enforce in spaces before NTIA negotiations really commence. This approach would better work for more established industries, however, since FTC regulation in a very new area risks being unattached to industry standards. The paradox is that if an industry is particularly new, there won't yet be industry standards for the FTC to enforce. Hence, the FTC may be

152. Harter describes, as a condition for reg neg regulatory negotiations, that parties cannot come into negotiations with fundamentally opposing values. Harter, *supra* note 130, at 19.

153. This Article leaves aside, for the moment, discussion of what level of both auditing and enforcement would ensure the efficacy of those privately negotiated safe harbors.

154. *See* Aaron Souppouris, *The EU-US Privacy Shield Is up, But It's Future Is in Doubt*, ENGADGET (July 12, 2016), https://www.engadget.com/2016/07/12/eu-us-privacy-shield-data-protection/; *see also* Klint Finley, *Privacy Shield Will Let U.S. Tech Giants Grab Europeans' Data*, WIRED (July 12, 2016, 7:03 PM).

155. *See* Rubinstein, *supra* note 35, at 401 (describing the GNI covenanting process as occurring in the shadow of proposed regulation).

ill-equipped to create the penalty default against which the NTIA can encourage negotiations in these new technological spaces.

So perhaps the bigger lesson is that the NTIA process is, under current U.S. privacy law, particularly unsuited to exactly the task to which it has been assigned: to drive negotiations by private actors and stakeholders in emerging industries, before other government entities are equipped to contemplate regulations. The NTIA process, paradoxically, may be better suited to application in areas where the FTC or states have already created enforcement mechanisms. Its information-drawing and negotiation-driving functions, given the current lack of U.S. federal data privacy law, are limited. For the NTIA process to work as contemplated—for it to effectively pull both information and expertise from private actors—the United States must establish an effective privacy penalty default.

CONCLUSION

In the absence of federal data privacy law, the White House has employed the NTIA to engage in a version of co-regulation of privacy in three nascent sectors. That process has largely failed. The government's motives of wanting to involve private expertise in the process are sound; the regulatory backdrop to the process, however, is ineffective. If the United States wants to engage in co-regulation in data governance, we must create a penalty default that makes it more palatable for private actors to engage in this type of co-regulation. Among the many reasons for enacting federal data privacy law, I here add another: well-crafted federal data privacy law may be essential for exactly the kind of co-regulation that our government envisions. In the meantime, reliance on the substance of the NTIA's output for constructing regulation is ill-advised.