2016

Friending the Privacy Regulators

William McGeveran
University of Minnesota Law School, billmcg@umn.edu

FRIENDING THE PRIVACY REGULATORS

William McGeveran*

According to conventional wisdom, data privacy regulators in the European Union are unreasonably demanding, while their American counterparts are laughably lax. Many observers further assume that any privacy enforcement without monetary fines or other punishment is an ineffective "slap on the wrist." This Article demonstrates that both of these assumptions are wrong. It uses the simultaneous 2011 investigations of Facebook's privacy practices by regulators in the United States and Ireland as a case study. These two agencies reached broadly similar conclusions, and neither imposed a traditional penalty. Instead, they utilized "responsive regulation," where the government emphasizes less adversarial techniques and considers formal enforcement actions more of a last resort.

When regulators in different jurisdictions employ this same responsive regulatory strategy, they blur the supposedly sharp distinctions between them, despite what may be written in their respective constitutional proclamations or statute books. Moreover, "regulatory friending" techniques work effectively in the privacy context. Responsive regulation encourages companies to improve their practices continually, it retains flexibility to deal with changing technology, and it discharges oversight duties cost-effectively, thus improving real-world data practices.

TABLE OF CONTENTS

---

* Associate Professor and Solly Robins Distinguished Research Fellow, University of Minnesota Law School. I am grateful for helpful comments and support from Anupam Chander, Jessica Clarke, Julie Cohen, Woodrow Hartzog, Kristin Hickman, Dennis Hirsch, Chris Hoofnagle, Margot Kaminski, Paul Ohm, Neil Richards, Mary Rumsey, Daniel Schwarcz, and David Thaw. Earlier drafts of this paper were presented at the Privacy Law Scholars Conference, hosted by UC Berkeley School of Law; the Midwestern Privacy Workshop, hosted by Notre Dame Law School; and workshops at Yale Law School, the University of Iowa College of Law, and the University of Minnesota Law School. I also benefited from work completed as a visiting professor at University College Dublin Sutherland School of Law, and I am indebted to Colin Scott, Gavin Barrett, Imelda Maher, and T.J. McIntyre for their assistance and hospitality there. Finally, thanks to my exceptional student research assistants, Chelsea Lemke and Hannah Nelson.

INTRODUCTION

At the end of 2011, two different government privacy regulators completed comprehensive investigations of the social networking platform Facebook. Both reached broadly similar conclusions about the data-handling practices they examined. Rather than imposing a conventional penalty, both regulators reached agreements with the company compelling numerous improvements in the treatment of personal data. This Article uses the Facebook investigations as a case study of global privacy enforcement today.

The approach taken by both of these regulators was a textbook illustration of a form of new governance theory known as "responsive regulation," which has a long pedigree in administrative law scholarship. Using this model, the government emphasizes less adversarial techniques and only turns to formal and punitive enforcement actions as a last resort if these fail. The Facebook case study illustrates how these techniques have been adapted to privacy law. In effect, Facebook and the privacy regulators "friended" one another.

This Article argues that we should understand most privacy regulation through the prism of responsive regulation. Doing so illuminates two important features of enforcement practices.

First, the two Facebook investigations reached similar outcomes even though they occurred in two different countries with considerably divergent bodies of substantive law. In the United States, Facebook came under the scrutiny of the Federal Trade Commission ("FTC" or the "Commission"), which is a consumer protection agency, not primarily a privacy regulator. The other investigation was conducted by the Office of the Data Protection Commissioner ("ODPC") in the Republic of Ireland. Unlike the consumer protection law underlying the FTC's authority, the ODPC enforces a data protection regime. The consumer protection

approach dominant in the United States and the data protection approach used throughout the European Union ("E.U.") differ greatly in substance and emphasis.[1] But the use of responsive regulation on both sides of the Atlantic blurs the supposedly sharp distinctions between jurisdictions, whatever may be written in their respective constitutional proclamations or statute books.

Second, responsive regulation works pretty well. Some observers, particularly in continental Europe, have criticized privacy enforcement in Ireland as too permissive.[2] Austrian privacy advocate Max Schrems once dubbed Ireland "the Cayman Islands of the data barons."[3] U.S. regulators are often subject to similar disparagement when they close enforcement actions without imposing traditional punishments.[4] But the well-established literature on new governance methods, including responsive regulation, demonstrates that tough and punitive enforcement is not the true indicator of effective law.[5] Where prior literature typically focused on more industrial-era issues such as pollution control and product safety,[6] this Article confirms that the model fares well in the digital economy too. "Regulatory friending" is especially well suited to the privacy context. It gives companies more

---

1. *See infra* Part I.

2. *See* Ian Burrell, *Billy Hawkes: The Irishman with a Billion People's Privacy to Protect*, INDEPENDENT (Feb. 7, 2014), http://www.independent.co.uk/life-style/gadgets-and-tech/news/billy-hawkes-the-irishman-with-a-billion-people-s-privacy-to-protect-9115818.html.

> Joe McNamee of European Digital Rights (EDRi), a civil rights group, says the Irish commissioner's office has 'little credibility.' Privacy advocates accuse it of practising light-touch regulation. The Irish DPC allows companies to 'do whatever they want with personal data,' plays down the threat of sanctions, and rarely uses enforcement powers, says EDRi.

Leo Mirani, *How a Bureaucrat in a Struggling Country at the Edge of Europe Found Himself Safeguarding the World's Data*, QUARTZ (Jan. 7, 2014), http://qz.com/162791/how-a-bureaucrat-in-a-struggling-country-at-the-edge-of-europe-found-himself-safeguarding-the-worlds-data/.

3. Derek Scally, Opinion, *High Court Privacy Case Puts Ireland at Centre of Data Collection Controversy*, IRISH TIMES (June 14, 2014, 12:01 AM), http://www.irishtimes.com/business/technology/high-court-privacy-case-puts-ireland-at-centre-of-data-collection-controversy-1.1831895.

4. For example, one technology blogger reacted angrily to a settlement the FTC reached with the makers of the popular social messaging app Snapchat, protesting that "[t]he Federal Trade Commission today effectively told technology companies: Go ahead and lie to consumers about your privacy protections, because even if you get caught, the most you'll have to do is apologize. (If that.)" Selena Larson, *FTC To Silicon Valley: Lying About User Privacy Will Get You a Big . . . Wrist Slap*, READWRITE (May 8, 2014), http://readwrite.com/2014/05/08/snapchat-ftc-wrist-slap-user-privacy.

5. *See infra* Part II (discussing influential new governance scholarship that deemphasizes the primacy of punitive measures).

6. *See, e.g.*, REGULATORY ENCOUNTERS (Robert A. Kagan & Lee Axelrad eds., 2000) (discussing the distinction between adversarial regulation and more cooperative forms of new governance, and collecting articles analyzing how these techniques are applied in different countries to regulate the environment, employment, and product safety).

clarity about their compliance obligations and minimizes their risk of being surprised by an adversarial regulatory action in a fast-changing environment. Meanwhile, regulators can improve real-world data practices efficiently, flexibly, and cooperatively. Since the 2011 investigations, Facebook has greatly improved its treatment of personal data, and in certain ways its policies are now exemplary.[7]

An assessment of responsive privacy regulation across the United States and the E.U. is very timely at this moment for several reasons.

To begin with, in recent years, the ODPC has become one of the world's most important privacy regulators. Facebook, Inc. manages its relationship with all users outside the United States and Canada through Facebook Ireland Ltd., its Dublin-based subsidiary.[8] For reasons mostly unrelated to privacy,[9] numerous other global technology companies have also established substantial second homes in Ireland, including Google, Apple, Intel, Twitter, and eBay.[10] That puts the ODPC at the center of the most cutting-edge digital privacy issues. Yet, there has been little sustained scholarly scrutiny of Irish privacy law or the ODPC.

Meanwhile, E.U. data protection law, and therefore Irish law along with it, is changing rapidly. In late 2015, an E.U. court case invalidated the U.S.–E.U. Safe Harbor Agreement, a legal mechanism used by over 4,500 U.S. companies to transfer personal data from the E.U. to the United States—potentially subjecting many more of them to E.U. enforcement.[11] A replacement mechanism, known as the "Privacy Shield," went into effect in mid-2016, but remains untested.[12] Also in

---

7. *See infra* notes 338–42 and accompanying text (discussing Facebook's privacy improvements since 2011).

8. *See infra* notes 317–19 and accompanying text (discussing Facebook's significant presence in Ireland).

9. *See infra* notes 194–97 and accompanying text (discussing reasons technology companies like Facebook have located in Ireland).

10. According to one industry group, "At the last count, 179 companies from the [U.S.] West Coast were employing over 36,000 people in Ireland—among them PayPal, Twitter, Apple, Intel, eBay, Qualcomm, Oracle, McAfee and Yahoo!." Thomas Breathnach, *Silicon Docklands to Silicon Valley*, MAKE IT IN IR. (Apr. 2, 2014), http://makeitinireland.com/silicon-docklands-to-silicon-valley.

11. Not incidentally, the case centered on Ireland's ODPC. *See* Case C-362/14, Schrems v. Data Prot. Comm'r, 2015 EUR-Lex CELEX LEXIS 614CJ0362 (Oct. 6, 2015); Mark Scott, *Data Transfer Pact Between U.S. and Europe Is Ruled Invalid*, N.Y. TIMES (Oct. 6, 2015), http://www.nytimes.com/2015/10/07/technology/european-union-us-data-collection.html.

12. European Commission Press Release IP/16/2461, European Commission Launches EU-U.S. Privacy Shield: Stronger Protection for Transatlantic Data Flows (July 12, 2016), http://europa.eu/rapid/press-release_IP-16-2461_en.htm; Natalia Drozdiak, *EU Privacy Regulators Give Green Light to Data-Transfer Pact With U.S.*, WALL ST. J. (July 26, 2016, 9:33 AM), http://www.wsj.com/articles/eu-privacy-regulators-give-green-light-to-data-transfer-pact-with-u-s-1469534432 (reporting qualified approval of Privacy Shield by Article 29 Working Party, which is composed of national data protection authorities); Sean Hargrave, *Is Privacy Shield Already A Dead Man Walking?*, MEDIAPOST (July 27, 2016, 10:24 AM), http://www.mediapost.com/publications/article/281233/is-privacy-shield-

2016, the E.U. officially adopted its new General Data Protection Regulation ("GDPR"), the most comprehensive overhaul of E.U. privacy rules in over two decades.[13] The revisions move European statutory law even further from the U.S. approach and create enormous new potential fines—but leave most day-to-day power in the hands of the same national regulators as before.[14] Understanding the significance of regulatory style will be crucial to assessing the impact of the new GDPR, which will become effective in all E.U. countries, including Ireland, in 2018.

Finally, this Article is timely because U.S. privacy scholarship has recently taken an administrative turn that more closely examines the actual enforcement of privacy law.[15] More academic authors have begun to emphasize data handling "on the ground"[16] and to challenge the oversimplified picture of a vast transatlantic gulf

---

already-a-dead-man-walking.html (expressing skepticism about long-term survival of Privacy Shield).

13. Commission Regulation 2016/679, 2016 O.J. (L 119) 1, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679 [hereinafter GDPR]; *see* European Commission Press Release IP/15/6321, Agreement on Commission's EU Data Protection Reform Will Boost Digital Single Market (Dec. 15, 2015), http://europa.eu/rapid/press-release_IP-15-6321_en.htm; *Data Protection Reform-Parliament Approves New Rules Fit For the Digital Era*, EUR. PARLIAMENT: NEWS (Apr. 14, 2016, 12:11 PM), http://www.europarl.europa.eu/news/en/news-room/20160407IPR21776/data-protection-reform-parliament-approves-new-rules-fit-for-the-digital-era; Mark Scott, *Europe Approves Tough New Data Protection Rules*, N.Y. TIMES (Dec. 15, 2015), http://www.nytimes.com/2015/12/16/technology/eu-data-privacy.html.

14. For further discussion of the GDPR, see *infra* notes 52–53 and accompanying text and notes 398–400 and accompanying text.

15. *See, e.g.*, ENFORCING PRIVACY: REGULATORY, LEGAL, AND TECHNOLOGICAL APPROACHES (David Wright & Paul De Hert eds., 2016) [hereinafter ENFORCING PRIVACY] (collecting international scholarship on governance and privacy law); CHRIS JAY HOOFNAGLE, FEDERAL TRADE COMMISSION PRIVACY LAW AND POLICY (2016) (examining FTC regulation of consumer privacy); Francesca Bignami, *Cooperative Legalism and the Non-Americanization of European Regulator Styles: The Case of Data Privacy*, 59 AM. J. COMP. L. 411 (2011) (comparing data privacy regulation in four countries); Danielle Keats Citron, *Privacy Policymaking of State Attorneys General*, 92 NOTRE DAME L. REV. (forthcoming 2016), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2733297 (analyzing privacy enforcement by state attorneys general); Julie E. Cohen, *The Regulatory State in the Information Age*, 17 THEORETICAL INQUIRIES L. 369 (2016) (arguing administrative regulation has changed to become informal, financialized, and involving increased input from the private sector); Dennis D. Hirsch, *The Law and Policy of Online Privacy: Regulation, Self-Regulation, or Co-Regulation?*, 34 SEATTLE U.L. REV. 439 (2011) (comparing regulatory models available for privacy enforcement); Justin (Gus) Hurwitz, *Data Security and the FTC's UnCommon Law*, 101 IOWA L. REV. 955 (2016) (critiquing FTC's enforcement techniques in data security cases); Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583 (2014) (arguing that privacy attorneys and the FTC treat consent decrees like an emerging "common law of privacy"); David Thaw, *The Efficacy of Cybersecurity Regulation*, 30 GA. ST. U.L. REV. 287 (2014) (using empirical methods to evaluate different regulatory techniques applied to private-sector cybersecurity practices).

16. *See, e.g.*, KENNETH A. BAMBERGER & DEIRDRE K. MULLIGAN, PRIVACY ON THE GROUND: DRIVING CORPORATE BEHAVIOR IN THE UNITED STATES AND EUROPE (2015);

between U.S. and E.U. law in practice.[17] While there was earlier privacy law scholarship in this vein, most notably the classic work of Colin Bennett (alone and with co-author Charles Raab),[18] serious examination of regulatory enforcement has increased considerably in the last three to five years. By systematically analyzing responsive regulation as a framework to describe multiple countries' enforcement, this Article contributes to an emerging privacy literature that grapples with the mechanisms that turn abstract rules into real-world practices.[19]

This Article proceeds as follows. Part I provides the legal background that shows how the "data protection" model in the E.U. (and specifically Ireland) differs from the "consumer protection" model more common in U.S. privacy law. Part II introduces the concept of responsive regulation from administrative law scholarship. Part III then explores the application of the responsive regulation model to day-to-day enforcement of privacy law in the United States and Ireland. Part IV gets more specific, examining the Facebook investigations as an example of responsive regulation in action. Finally, in Part V, this Article concludes by identifying lessons that can guide policy development and further study.

The significance of responsive regulation should not be overstated. The considerable differences between E.U. and U.S. privacy law described in Part I remain, despite the shared regulatory techniques discussed later in the Article. Moreover, while the privacy regulators examined here have adopted responsive techniques, others have chosen varying regulatory styles.[20] And responsive

---

Kenneth A. Bamberger & Deirdre K. Mulligan, *Privacy on the Books and on the Ground*, 63 STAN. L. REV. 247 (2011).

17. *See, e.g.*, Paul M. Schwartz, *The EU-US Privacy Collision: A Turn to Institutions and Procedures*, 126 HARV. L. REV. 1966 (2013) (applying Anne-Marie Slaughter's theory of international "harmonization networks" to show how U.S. and E.U. institutions have engaged each other in a collaborative process of informal lawmaking to bring their distinct privacy regimes into closer alignment); Solove & Hartzog, *supra* note 15, at 586 (arguing that, because of FTC's increased privacy enforcement, "such comparisons are increasingly becoming outdated"). *See generally* Christopher Wolf, *Delusions of Adequacy? Examining the Case for Finding the United States Adequate for Cross-Border EU-U.S. Data Transfers*, 43 WASH. U. J.L. & POL'Y 227, 243–50 (2014) (suggesting that U.S. privacy law might properly be deemed to offer the "adequate level of protection" for personal data required for cross-border transfers under E.U. law).

18. *See* COLIN J. BENNETT, REGULATING PRIVACY: DATA PROTECTION AND PUBLIC POLICY IN EUROPE AND THE UNITED STATES (1992); COLIN J. BENNETT & CHARLES D. RAAB, THE GOVERNANCE OF PRIVACY (2003); *see also* Steven Hetcher, *The FTC as Internet Privacy Norm Entrepreneur*, 53 VAND. L. REV. 2041 (2000); Jeff Sovern, *Protecting Privacy with Deceptive Trade Practices Legislation*, 69 FORDHAM L. REV. 1305 (2001). For a classic work on the formulation of privacy legislation rather than its regulatory enforcement, see PRISCILLA M. REGAN, LEGISLATING PRIVACY: TECHNOLOGY, SOCIAL VALUES, AND PUBLIC POLICY (1995).

19. A new examination by Graham Greenleaf engages in a somewhat comparable analysis of responsive privacy regulation in Asia. Graham Greenleaf, *Responsive Regulation of Data Privacy: Theory and Asian Examples*, in ENFORCING PRIVACY, *supra* note 15, at 233.

20. *See, e.g.*, Artemio Rallo Lombarte, *The Spanish Experience of Enforcing Privacy Norms: Two Decades of Evolution from Sticks to Carrots*, in ENFORCING PRIVACY, *supra* note 15, at 123, 131–141 (describing shift in Spanish data protection regulation from a

regulation certainly is not some panacea for effective privacy enforcement. Rather, regulators typically need to combine various strategies in different situations. All enforcement is imperfect: the rules will always be violated by some.

Nonetheless, the fact that authorities in Ireland and the United States can behave so similarly when enforcing such different laws belies the caricature of radical difference. This Article offers a more refined portrait: on both sides of the Atlantic, some regulators are moving toward pragmatic and flexible governance of data practices for the digital age. In the end, responsive regulation might be the most effective approach for protecting privacy while enjoying the benefits of technological development. Thus, the equivalent results often reached in Ireland and the United States are not problematic—they are desirable. Like any good friendship, responsive regulation benefits both parties.

I. DATA PROTECTION AND CONSUMER PROTECTION

Americans and Europeans view personal identity differently,[21] and therefore, they understand individuals' rights over the handling of their personal data differently too. Attorneys in the United States and the E.U. do not even use the same words to describe the law that governs the handling of personal information. Americans include it under the broad rubric of "privacy law," but E.U. and Irish sources consistently refer to it as "data protection law," a defined subset of a larger notion of privacy.[22] This difference extends far beyond nomenclature—it reflects values. I have used this difference in terminology to provide students and practitioners with helpful shorthand for two distinctive models of privacy rules.[23] Europe uses the "data protection" model. In the United States, a "consumer protection" model dominates privacy law.

These distinctions have long and strong roots, extending back to antecedents such as continental European social structures based on honor, dignity, and rank on one side, and the New World's individualistic spirit on the other.[24] Ireland can be seen as something of a hybrid: it is an island isolated from some historical currents and a part of the Anglo-American legal and political culture, but it shares Europe's formal regulatory structure (by virtue of E.U. membership) as

---

highly punitive fine-oriented structure to one that includes warning letters for first offenses and other more graduated responses).

21. Indeed, they view many things differently. *See generally The American-Western European Values Gap*, PEW RES. CTR. (Feb. 29, 2012), http://www.pewglobal.org/2011/11/17/the-american-western-european-values-gap/.

22. *See* CHRISTOPHER KUNER, EUROPEAN DATA PROTECTION LAW: CORPORATE COMPLIANCE AND REGULATION 2–3 (2d ed. 2007). Bennett argues that the "data protection" nomenclature is preferable because it is more precise. *See* BENNETT, *supra* note 18, at 12–14.

23. *See generally* WILLIAM MCGEVERAN, PRIVACY AND DATA PROTECTION LAW 165–323 (2016).

24. *See* James Q. Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, 113 YALE L.J. 1151 (2004).

well as much of the continent's long feudal and clannish history.[25] The differing rules in the United States and in Ireland reflect these distinct histories.

The "data protection" model characterizes law in all E.U. member states, including Ireland. As discussed below, data protection law begins with an assumption that control over personal information is a human right.[26] This generally leads, in turn, to particular types of rules, including more specific terms and broader prerogatives for individuals.[27] On the other side of the ocean, generally applicable American privacy law embraces a "consumer protection" approach.[28] U.S. regulators, such as the FTC or state attorneys general, regulate privacy by policing the fairness of particular transactions, much as they do when safeguarding individuals against price gouging or false advertising.[29]

All E.U. nations have adopted comprehensive data protection legislation overseen by specialized data protection authorities ("DPAs"), while U.S. privacy law is more piecemeal—many sectoral statutes that concern only certain subject areas or particular technologies. Some of these narrower U.S. regulations are properly described as data protection regimes, rather than consumer protection regimes. These include regulations propagated by the Health Insurance Portability and Accountability Act ("HIPAA")[30] and the Children's Online Privacy Protection Act ("COPPA").[31] However, these are exceptions to the general pattern in the United States; they were adopted only to protect especially sensitive data in defined and highly regulated areas. There are a few sectoral laws in the E.U. as well,[32] but they all adhere to data protection principles.

This Part explains more fully the differences between the data protection and consumer protection models. But first I want to highlight what is probably the most significant of these differences: the default rule. A consumer protection regime generally allows any collection and processing of personal data, unless it is specifically forbidden. Data protection law adopts the opposite default, permitting collection and processing only for a statutorily defined justification. In other words: in the United States, it is usually allowed unless the law says that it is not, while in the E.U. it is not allowed unless the law says that it is.[33]

Because of this and other distinctions between data protection and consumer protection law, an observer who simply examined this paper record—

---

25. *See generally* RICHARD KILLEEN, A BRIEF HISTORY OF IRELAND (2012).
26. *See infra* notes 38–43 and accompanying text.
27. MCGEVERAN, *supra* note 23, at 257–58.
28. *See infra* notes 110–16 and accompanying text.
29. *See* MCGEVERAN, *supra* note 23, at 165.
30. Pub. L. No. 104-191 (1996) (codified in scattered sections of 29 U.S.C.; 42 U.S.C.; 26 U.S.C.; 18 U.S.C.); *see also* 45 C.F.R. § 164 (2016).
31. 15 U.S.C. §§ 6501–06; *see* 16 C.F.R. § 312 (2016).
32. *See* BENNETT & RAAB, *supra* note 18, at 105–06.
33. *See* MCGEVERAN, *supra* note 23, at 257.

perhaps the proverbial visiting Martian[34]—might think the United States and the E.U. were different planets when it comes to privacy law. Before the rest of the Article turns to the analysis of convergence in enforcement, this initial Part reviews the divergence in formal rules and underlying motivations. It will first consider data protection rules found in Ireland and the E.U., and then the consumer protection model that dominates U.S. privacy law. This discussion will also provide background information that is important for understanding the discussion of responsive regulation in the remainder of the Article.

A. The European Data Protection Model

European legal sources tend to view control over personal data as an inherent aspect of individual dignity. This concept can be attributed in part to continental political and cultural development of the idea that personal reputation and honor are central to human flourishing.[35] Other distinctive European legal doctrines, such as moral rights in intellectual property law, have similar origins.[36] Some analysts suggest that the memory of twentieth-century totalitarian governments—which compiled personal data to facilitate atrocities such as the Nazi Holocaust, the Stalinist purges, and political repression in Warsaw Pact countries—may also explain reverence for data protection in Europe.[37] All of these historical experiences probably contribute to the E.U.'s treatment of data protection rights today.

Multiple European constitutional documents and treaties name privacy as a fundamental human right, explicitly equivalent to other essential rights such as freedom of expression or the entitlement to a fair trial.[38] This treatment is clearly evident in the Charter of Fundamental Rights, the closest thing to an E.U.

---

34. *See* Riley v. California, 134 S. Ct. 2473, 2484 (2014) ("[M]odern cell phones . . . are now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy.").

35. *See* Whitman, *supra* note 24, at 1164–89 (tracing the emergence of privacy rights from continental European concepts of honor and dignity); *see also* G.A. Res. 217 (III) A, Universal Declaration of Human Rights, art. XII (Dec. 10, 1948) ("No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation.").

36. *See generally* Sonya G. Bonneau, *Honor and Destruction: The Conflicted Object in Moral Rights Law*, 87 ST. JOHN'S L. REV. 47, 53–54 (2013).

37. *See* Kenneth A. Bamberger & Deirdre K. Mulligan, *Privacy in Europe: Initial Data on Governance Choices and Corporate Practices*, 81 GEO. WASH. L. REV. 1529, 1618 (2013); Joel R. Reidenberg, *Resolving Conflicting International Data Privacy Rules in Cyberspace*, 52 STAN. L. REV. 1315, 1349–50 (2000).

38. *See, e.g.*, Council of Europe, European Convention on Human Rights, Art. 8(1), Sept. 3, 1953, 213 U.N.T.S. 222 ("Everyone has the right to respect for his private and family life, his home and his correspondence."); G.A. Res. 217 (III) A, *supra* note 35 ("No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation.").

constitutional bill of rights,[39] as well as the European Convention on Human Rights, of which Ireland is a signatory (as are all other E.U. nations).[40] These documents enshrine positive rights based on dignity and honor that are generally enforceable against non-state actors. For example, individuals can invoke privacy rights guaranteed by the European Convention or the E.U. Charter in support of lawsuits against newspapers or magazines that allegedly invaded their privacy.[41]

The Irish Constitution (like its U.S. counterpart) does not recognize an explicit right to privacy or data protection in so many words, but Irish courts (like U.S. ones) have inferred general privacy rights from other constitutional text and structure. [42] Substantively, however, the resulting inferences from Ireland's constitutional order resemble the privacy rights enshrined more directly in other European constitutions, rather than American constitutional privacy. As summarized by a pair of Trinity College legal scholars, "[t]he Irish courts have consistently described the right to privacy in a way which emphasises its connection with dignitary values."[43] Regardless of the interpretation of the Republic of Ireland's constitution, the country is also subject to the provisions of the European Convention and, when implementing E.U. law, the Charter. Thus, European and Irish

---

39. Article 8 of the Charter reads:

> Protection of personal data
>
> 1. Everyone has the right to the protection of personal data concerning him or her.
>
> 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
>
> 3. Compliance with these rules shall be subject to control by an independent authority.

Charter of Fundamental Rights of the European Union, 2012 O.J. (C326) 391, 397.

40. European Convention on Human Rights *supra* note 38. Adherence to the Convention is entirely separate from E.U. membership. Plenty of countries that do not belong to the E.U. are signatories of the Convention; the United Kingdom's planned withdrawal from the E.U. would not itself change its status as a Convention signatory. Katie Grant, *What Does Brexit Mean For Our Human Rights?*, iNEWS (June 24, 2016, 5:37 PM), https://inews.co.uk/essentials/news/uk/brexit-means-human-rights/.

41. *See, e.g.*, Mosley v. News Grp. Newspapers Ltd., [2008] EWHC (Q.B.) 1777 (Eng.); Von Hannover v. Germany, 2004-VI Eur. Ct. H.R. 294; Axel Springer AG v. Germany (No. 2), EUR. CT. HUMAN RTS. (Oct. 10, 2014), http://hudoc.echr.coe.int/eng?i=001-145700.

42. *See, e.g.*, Caldwell v. Mahon [2006] IEHC 86 (H. Ct.) (Ir.); Kennedy v. Ireland [1987] IR 587 (Ir.); Norris v. Attorney General, [1984] I.R. 36 (SC) (Ir.).

43. HILARY DELANY & EOIN CAROLAN, THE RIGHT TO PRIVACY 37 (2008) ("Irish constitutional law rejected the traditional Anglo-American conception of privacy as a narrow interest in isolation or inaccessibility in favour of a more sophisticated understanding of privacy as a relational right."). The authors' discussion tracing the historical development of Irish constitutional privacy jurisprudence can be found at *id*. at 33–56.

constitutional law combine to establish control over personal data as a human right of the highest order.

Statutory enactments in Europe and Ireland protect these rights with a robust data protection regime. For the last several decades, the central statutory instrument in the E.U. has been the Data Protection Directive of 1995 ("the Directive"),[44] which was promulgated just as the commercial development of the internet was set to explode with the spread of web browsers.[45] The Directive sought to harmonize data protection law throughout the E.U., consistent with the Union's broader goal of removing obstacles to free trade and movement between member states.[46] While it aimed for uniformity, the Directive also set a relatively stringent baseline for substantive data protection around which countries would coalesce.[47] Article 1 of the Directive sets out these twin goals directly.[48]

Like all E.U. directives, the Data Protection Directive compelled member states to enact domestic legislation consistent with its terms. It left some margin for different implementations on certain points, including many enforcement decisions, but it also set minimum requirements for national law.[49] In 1988, before the Directive, Ireland had already enacted a comprehensive Data Protection Act.[50] In 2003, the Irish Parliament amended the 1988 Act to reconcile a few remaining inconsistencies between the statute and the Directive.[51]

---

44. *See* Directive 95/46/EC, of the European Parliament and of the Council on 24 Oct. 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 OJ (L281) 31 [hereinafter E.U. Data Protection Directive].

45. The first web browser, Mosaic, was released in 1993. The year of the Directive, 1995, was also when Microsoft introduced its groundbreaking Internet Explorer browser, and the year both Amazon and eBay were founded. *See Fifteen Years of the Web*, BBC NEWS (Aug. 5, 2006), http://news.bbc.co.uk/2/hi/technology/5243862.stm.

46. *See* Consolidated Version of the Treaty on the Functioning of the European Union pmbl., Oct. 26, 2012, 2012 O.J. (C 326) 47.

47. Schwartz, *supra* note 17, at 1973–74 (describing how Member States passed omnibus legislation to satisfy the Directive's requirements).

48. As the Directive says:

> 1. In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data.
>
> 2. Member States shall neither restrict nor prohibit the free flow of personal data between Member States for reasons connected with the protection afforded under paragraph 1.

E.U. Data Protection Directive, *supra* note 44, at art. 1.

49. *See* KUNER, *supra* note 22, at 34–35 (describing the supremacy of E.U. law and implementation of directives).

50. Data Protection Act, (Act No. 25/1988) (Ir.), http://www.irishstatutebook.ie/1988/en/act/pub/0025/index.html [hereinafter Irish Data Protection Act 1988].

51. Data Protection Act 2003 (Act No.6/2003) (Ir.), http://www.irishstatutebook.ie/2003/en/act/pub/0006/index.html [hereinafter Irish Data

When it takes effect in 2018, the GDPR will automatically become the law in Ireland and every other E.U. nation, supplanting the Directive and previous national data protection laws.[52] Because the GDPR is even stricter than the Directive and the Irish Act in every important respect, the upcoming change does not affect the analysis of responsive regulation in this Article, which only describes the formal data protection regime in broad strokes. Indeed, the GDPR leaves national data protection authorities in place as its primary enforcers even while making substantive law more restrictive. As a result, the new rules might *increase* the distance between the enactments written in the books by European functionaries and the actions of regulators acting on the ground in individual member-state capitals.[53]

Ireland's Data Protection Act is very faithful to the Directive, and the core provisions described here are close to the GDPR as well. Its central definitions are the broad categories of "personal data" and "processing."[54] According to the Act, personal data is "data relating to a living individual who is or can be identified."[55] As guidance from the ODPC explains, "The definition is—deliberately — a very broad one. In principle, it covers any information that relates to an identifiable, living individual."[56] This is exactly how the Directive defines personal data.[57] "Personally identifiable information" is a well-recognized category in privacy law; similar definitions are found in several U.S. data protection statutes, including the HIPAA regulations.[58]

Protection Act]. The Law Reform Commission has prepared an unofficial administrative consolidation of the 1988 and 2003 Acts. Law Reform Commission, *Data Protection Act 1988 Revised* (July 30 2016), www.lawreform.ie/_fileupload/RevisedActs/WithAnnotations/EN_ACT_1988_0025.PDF.

52. *See* European Commission Press Release MEMO/15/6385, Questions and Answers—Data Protection Reform (Dec. 21, 2015), http://europa.eu/rapid/press-release_MEMO-15-6385_en.htm; European Commission Press Release IP/15/6321, Agreement on Commission's EU Data Protection Reform Will Boost Digital Single Market (Dec. 15, 2015), http://europa.eu/rapid/press-release_IP-15-6321_en.htm.

53. That said, the GDPR also includes mechanisms to increase uniformity of regulatory choices in different member states. For more about the distribution of regulatory authority under the GDPR, see *infra* notes 400–01 and accompanying text.

54. Irish Data Protection Act *supra* note 51, § 1(a)(iv)–(v).

55. *Id.*

56. *What is Personal Data?* DATA PROTECTION COMMISSIONER, http://www.dataprotection.ie/docs/What-is-Personal-Data-/210.htm (last visited Oct. 8, 2016). *See generally* PETER CAREY, DATA PROTECTION: A PRACTICAL GUIDE TO IRISH AND EU LAW 12–17 (2010).

57. E.U. Data Protection Directive, *supra* note 44, at art. 2. ("'[P]ersonal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity[.]").

58. *See* 45 C.F.R. § 160.103 (2014) (defining "individually identifiable health information"). Some scholars have warned that the concept of "personally identifiable information" should be substantially revised. *See generally* Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701, 1704 (2010) (warning that increased access to data and greater computing power can facilitate

The Data Protection Act's definition of processing is, if anything, even more wide-ranging.[59] Almost all modern digital activities fall under its umbrella, including virtually any imaginable collection, use, manipulation, distribution, or storage of personal data.[60] Manual methods such as keeping documents in a filing cabinet are also covered, provided they hold personal data in a "relevant filing system."[61] The Act also defines various actors connected to personal data: a data subject is "an individual who is the subject of personal data"; a data controller "controls the contents and use of personal data"; and a data processor—in practice, often a data controller's subcontractor—"processes personal data on behalf of a data controller."[62] These roles span all industries and all types of personal information, and they include private individuals as well as government, commercial, and nonprofit organizations.[63]

With all these terms defined, the Data Protection Act next addresses the substantive obligations of data controllers and processors. In line with the default rule of a data protection model, the Act only allows processing of personal data on

---

the combination of disparate data points to identify seemingly anonymous users); 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 (2011) (arguing that privacy law needs a personally identifiable information component but it should be reworked). Nevertheless, it remains a core concept in much of privacy and data protection law, including not only the Directive but also the future GDPR. *See* European Commission Press Release MEMO/15/6385, Questions and Answers—Data Protection Reform, *supra* note 52.

59. The full definition reads:

> "[P]rocessing" of or in relation to information or data, means performing any operation or set of operations on the information or data, whether or not by automatic means, including—
>
> (a) obtaining, recording or keeping the information or data,
>
> (b) collecting, organising, storing, altering or adapting the information or data,
>
> (c) retrieving, consulting or using the information or data,
>
> (d) disclosing the information or data by transmitting, disseminating or otherwise making it available, or
>
> (e) aligning, combining, blocking, erasing or destroying the information or data[.]

Irish Data Protection Act, *supra* note 51, § 1(a)(v).

60. *See* CAREY, *supra* note 56, at 18–19 ("This definition of processing is very wide and it is probably without limit. It could include *anything* that could be done with data.").

61. Irish Data Protection Act, *supra* note 51, § 1(a)(i) (defining "manual data"); CAREY, *supra* note 56, at 10–11 (describing examples of "manual data" subject to the Data Protection Act).

62. Irish Data Protection Act 1988, *supra* note 50, § 1.

63. CAREY, *supra* note 56, at 17 (expanding on scope of covered "persons" in statute).

the basis of "legitimate processing conditions"[64] specifically listed in the statute.[65] These include affirmative consent of the data subject,[66] legitimate interests of the data processor,[67] and various public functions (most of which concern public sector data processing).[68] Regulators and courts in both the E.U. and Ireland generally construe these narrowly.[69] The Data Protection Act also defines a category of "sensitive personal data,"[70] which is subject to an additional list of conditions beyond those applicable to all other personal data.[71]

Data subjects enjoy rights of access to records about themselves, whether held by public or private entities.[72] They have a right to be informed whether a data collector holds their personal information, and to inspect that data.[73] In Ireland, data subjects may demand copies of their personal data for a maximum charge of €6.35.[74] The Directive also grants data subjects the right to request that an entity correct or

---

64. PAUL LAMBERT, DATA PROTECTION LAW IN IRELAND: SOURCES AND ISSUES 69 (2013).

65. Irish Data Protection Act, *supra* note 51, § 4(2A).

66. *Id*. § 4 (2A)(1)(a). This provision also allows for family members to give consent on behalf of minors or incapacitated persons. *Id*. The GDPR continues the recognition of the data subject's consent as a legitimizing condition, but imposes a stricter standard for how that consent can be secured. *See* GDPR, *supra* note 13, at art. 7.

67. Irish Data Protection Act, *supra* note 51, § 4(2A)(1)(d). The statute explicitly subordinates interests of the data processor to those of the data subject, so this legitimizing condition does not apply in cases where there is "prejudice to the fundamental rights and freedoms or legitimate interests of the data subject." *Id*.

68. *Id*. §4(2A)(1)(c). These are enumerated in broad terms including "the administration of justice" and "function[s] of a public nature." *Id*.

69. *See, e.g.*, Case C-212/13, Ryneš v. Úřad Pro Ochranu Osobních Údajů, 2014 EUR-Lex CELEX LEXIS 62013CJ0212 ¶¶ 29–30 (Dec. 11, 2014) ("Since the provisions of Directive 95/46, in so far as they govern the processing of personal data liable to infringe fundamental freedoms, in particular the right to privacy, must necessarily be interpreted in the light of the fundamental rights set out in the Charter, the exception provided for in the second indent of Article 3(2) of that directive must be narrowly construed.") (citation omitted); CAREY, *supra* note 56, at 39–46 (particularly ¶¶ 4-22, 4-34, 4-39, 4-44, and 4-47).

70. Irish Data Protection Act, *supra* note 51, § 1(a)(1) (including within the definition of "sensitive personal data" the following: racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, physical or mental health, sexual life, commission or alleged commission of any offense, and any related criminal proceedings including verdict or sentencing).

71. *Id*. § 4(2B)(1)(b); *see* CAREY, *supra* note 56, at 58 (distilling these into 13 distinct conditions).

72. For a summary, see LAMBERT, *supra* note 64, at 87–108.

73. *See* BENNETT & RAAB, *supra* note 18, at 98 (dividing access rights into four categories, including right to know that data is held and to review it, as well as rights to "correct or delete" and associated rights of redress).

74. Irish Data Protection Act, *supra* note 51, § 5; *see Data Protection (Fees) Regulation* (S.I. No. 347/1988) (Ir.), http://www.irishstatutebook.ie/eli/1988/si/347/made/en/print; *Accessing Your Personal Information*, DATA PROTECTION COMMISSIONER, https://www.dataprotection.ie/docs/Making-an-Access-Request/963.htm (last visited Oct. 29, 2016).

delete inaccurate or irrelevant personal information and to revoke previous consent for data processing.[75] In 2014, the E.U.'s highest court interpreted the Directive to stipulate that these prerogatives, in combination, allow data subjects to demand the removal of certain search engine links about themselves.[76] As of November 2016, Google had fielded 4,485 such requests from people in Ireland.[77]

The comprehensive Irish Data Protection Act, as is typical in the E.U., extends to all types of organizations, be they public or private, for-profit or non-profit. The single statute covers every industry and every type of data.[78] Special additional requirements apply to sensitive data, but these are integrated into the same underlying statute, not treated separately.[79] The Irish law also covers most types of data-handling activities; it uses expansive definitions of personal data, of the individuals protected by the law, and of its territorial scope.[80] While E.U. data protection regimes do contain exceptions, especially for governmental activities, their scope is still much broader than that of any privacy law in the United States.[81]

B. The American Consumer Protection Model

U.S. privacy law is a smorgasbord. In contrast to European omnibus data protection statutes, most American privacy legislation responds to narrowly defined problems and applies solely to the type of data connected with that problem.[82] Some statutes take aim at particular industries, such as providers of healthcare or cable television.[83] Others relate only to certain types of technology, such as the federal Wiretap Act[84] or state laws specifically forbidding spyware[85] or "upskirt"

---

75. E.U. Data Protection Directive, *supra* note 44, at art. 12.

76. Case C-131/12, Google Spain v. Agencia Española de Protección de Datos, 2014 EUR-Lex CELEX LEXIS 62012CJ0131 (May 13, 2014).

77. *See European Privacy Requests for Search Removals*, GOOGLE: TRANSPARENCY REP., https://www.google.com/transparencyreport/removals/europeprivacy/ (last visited Nov. 4, 2016) (select Ireland from drop-down menu).

78. LAMBERT, *supra* note 65, at 57 ("All organizations that collect and process personal data must comply with the obligations of the Irish data protection regime."); *see* E.U. Data Protection Directive, *supra* note 44, at art. 3 (defining broad scope for E.U. data protection law).

79. Irish Data Protection Act, *supra* note 51, § 4(2B).

80. *Id*. § 1.

81. *See* ORLA LYNSKEY, THE FOUNDATIONS OF EU DATA PROTECTION LAW 15–30 (2015).

82. *See* Francesca Bignami & Giorgio Resta, *Transatlantic Privacy Regulation: Conflict and Cooperation*, 78 L. & CONTEMP. PROBS. 231, 238 (2015); Paul M. Schwartz, *Preemption and Privacy*, 118 YALE L.J. 902, 908–10 (2009).

83. *See* Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191 (1996) (codified in scattered sections of 29 U.S.C.; 42 U.S.C.; 26 U.S.C.; 18 U.S.C.); Cable Communications Policy Act of 1984, Pub. L. No. 98-549, 98 Stat. 2779 (1984) (codified in scattered sections of 47 U.S.C.).

84. Wire and Electronic Communications Interception and Interception of Oral Communication Act, 18 U.S.C. §§ 2510–2522 (2012).

85. *See, e.g.*, CAL. BUS. & PROF. CODE §§ 22947–22947.6 (West 2016) (preventing unauthorized users from collecting and using information on another's computer

photography.[86] Some information, such as personal financial records, may fall under multiple regimes simultaneously.[87] State tort law adds further mandates.[88] Government behavior is controlled largely by distinct constitutional limitations, combined with a few specialized statutes that add requirements above those constitutional minimums.[89] Many of these rules are enforced by the judiciary rather than any administrative enforcement authority.[90]

A few of these sectoral statutes in the United States resemble E.U. data protection laws.[91] They turn on the nature of the underlying personal information and individuals' interests in it, rather than on the transaction between data subjects and organizations. Like their European counterparts, they typically permit only data processing that falls within a legitimizing condition, and some also grant rights of access.[92]

The scope of these American data protection laws is limited, however. Health privacy rules promulgated under HIPAA cover a defined category of individually identifiable "personal health information" and only bind "covered entities" (mostly health insurers and medical providers) and their subcontractors.[93]

---

in a variety of ways without consent); 720 Ill. Comp. Stat. Ann. 5/17-52.5 (West 2011) (outlawing a variety of activities classified as "computer fraud"); UTAH CODE ANN. §§ 13-40-301 to 13-40-303 (West 2016) (preventing unauthorized users from collecting and using information on another's computer in a variety of ways without consent).

86. *See, e.g.*, MASS GEN. LAWS ANN. ch. 272, § 105 (West 2014) (banning surreptitious nonconsensual photography of private areas of the body, in response to the use of hidden cameras to photograph under women's skirts in public places).

87. *See* Fair Credit Reporting Act, 15 U.S.C. §§ 1681–1681x (2012); Graham-Leach-Bliley Act, 15 U.S.C. §§ 6801–6809 (2012); Bank Secrecy Act, 31 U.S.C. § 5311–5332 (2012).

88. *See* RESTATEMENT (SECOND) OF TORTS ch. 28, §§ 652A–652E (AM. LAW INST. 1977). Common-law tort claims, while often pleaded, seldom address the issues connected with large-scale modern data processing. *See* Danielle Keats Citron, *Mainstreaming Privacy Torts*, 98 CAL. L. REV. 1805, 1826–28 (2010); *see also* Neil M. Richards & Daniel J. Solove, *Prosser's Privacy Law: A Mixed Legacy*, 98 CAL. L. REV. 1887, 1922–24 (2010).

89. *See* Privacy Act, 5 U.S.C. § 552a (2012); Electronic Communications Privacy Act, 18 U.S.C. §§ 2510–2712, 3121–3127 (2012).

90. That is true, naturally, of the common-law torts. It also describes almost all enforcement against privacy violations by government actors, whether constitutional or statutory. Because this Article concerns regulatory agencies' enforcement models, tort claims and restrictions against government activity fall outside its scope. But the existence of additional privacy rules beyond administrative regulations further demonstrates the fragmented nature of U.S. privacy law.

91. *See* MCGEVERAN, *supra* note 23, at 322–23 (listing and briefly describing several U.S. sectoral data protection statutes).

92. *See, e.g.*, Fair Credit Reporting Act, 15 U.S.C. § 1681b (listing permissible purposes of consumer report information); § 1681g (mandating disclosure of certain consumer records to consumers upon request).

93. *See* 45 C.F.R. §§ 160.102 (2016); Modifications to the HIPAA Privacy, Security, Enforcement and Breach Notification Rules; Other Modifications to the HIPAA Rules, 78 Fed. Reg. 5566, 5589 (Jan. 25, 2013).

Protection for children's privacy under COPPA[94] applies only to operators of online services like websites, and only when they have actual or constructive knowledge that they gather information from children under the age of 13.[95] The Fair Credit Reporting Act only regulates certain carefully defined dossiers of information that are intended for specified purposes, such as underwriting loans or insurance and screening employment applicants.[96] These specialized statutes leave undisturbed the U.S. default rule—data collection and processing is allowed unless a specific rule forbids it—because most activities are not subject to these narrow restrictions.

Constitutional privacy rights in the United States are also circumscribed. The U.S. Constitution is the oldest national written constitution in use today and is among the most difficult to amend.[97] Consequently, it says little about the modern concept of privacy and does not mention the word "privacy" at all. Generally, constitutional recognition of privacy in the United States is consistent with a more libertarian and less constitutive view of those rights. It is a highly American form of privacy, intended to keep the government out of citizens' lives. This familiar "right to be let alone"[98] was, according to Justice Brandeis, "the most comprehensive of rights and the right most valued by civilized men."[99]

Yet protection for this most comprehensive of rights in the U.S. Constitution[100] is not nearly as comprehensive as data protection rights in European constitutions. Privacy is generally subordinate to many other rights expressed more clearly in the constitutional text, most notably the First Amendment guarantee of free speech.[101]Furthermore, U.S. constitutional privacy protects individuals from

---

94. *See* 15 U.S.C. §§ 6501–6502 (2012); 16 C.F.R. §§ 312.2, 312.3 (2016).

95. *See* 16 C.F.R. §§ 312.2, 312.3 (2016).

96. *See* 15 U.S.C. § 1681b.

97. *See* Elai Katz, *On Amending Constitutions: The Legality and Legitimacy of Constitutional Entrenchment*, 29 COLUM. J.L. & SOC. PROBS. 251, 260–61 (1996).

98. For early uses of the phrase, see THOMAS COOLEY, A TREATISE ON THE LAW OF TORTS, OR, THE WRONGS WHICH ARISE INDEPENDENT OF CONTRACT 29 (2d ed. 1888); Samuel D. Warren & Louis Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 193 (1890).

99. Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting).

100. A number of U.S. state constitutions enumerate a more specific privacy right than does the federal constitution. Only one of them, California, confers anything like a data protection right, or any right against private actors. *See* CAL. CONST., art. 1, §1; Hill v. Nat'l Collegiate Athletic Ass'n., 865 P.2d 633, 644 (Cal. 1994). However, the test for suits under this California constitutional provision is rigorous: "The party claiming a violation of the constitutional right of privacy established in article I, section 1 of the California Constitution must establish (1) a legally protected privacy interest, (2) a reasonable expectation of privacy under the circumstances, and (3) a serious invasion of the privacy interest." International Federation of Professional & Technical Engineers, Local 21 v. Superior Court, 165 P.3d 488, 499 (Cal. 2007).

101. The boundaries between these two are highly contested in the scholarly literature. *Compare*, Eugene Volokh, *Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People from Speaking About You*, 52 STAN. L. REV. 1049 (2000) (arguing that most privacy laws present possible conflicts with the First Amendment), *with* NEIL RICHARDS, INTELLECTUAL PRIVACY: RETHINKING CIVIL LIBERTIES IN

snooping or meddling by the government, but it does not constrain a person (or private business) from collecting or using information about others, nor does it confer human rights on individuals to control their personal data.[102] It is, to borrow from Isaiah Berlin, a negative liberty rather than a positive one.[103]

Of course, modern courts have read various privacy protections into their constitutional interpretations. The Fourth Amendment protects privacy not only from law enforcement searches[104] but against unreasonable intrusions in public schools[105] and government workplaces[106] as well. A line of cases under the doctrine of substantive due process protects "decisional privacy" in intimately personal matters.[107] Even the First Amendment generates privacy rights necessary to exercise the fundamental freedoms protected there.[108]

This constitutional jurisprudence does not confer any broad right to control personal information equivalent to European human rights to data protection. U.S. constitutional rights protect individuals from government interference—for example, from unreasonable searches[109] or limits on autonomous personal choices.[110] The Supreme Court had explicit opportunities to identify a substantive constitutional right to data protection three times, but each time it declined to do so.[111] In *Whalen v. Roe*, the Supreme Court accepted only that a duty to safeguard citizen data in government databases "*arguably* has its roots in the Constitution,"[112] and lower courts have been divided and inconsistent in their recognition of even the narrowest version of this right.[113]

THE DIGITAL AGE 86–90 (2014) (arguing that most privacy laws are consistent with the First Amendment).

102. *See* DeShaney v. Winnebago Cty. Dept. of Soc. Servs., 489 U.S. 189, 195–96 (1989) (holding that constitutional rights limit state action, but do not compel the government to restrain private actors from conduct). *See generally* Richard S. Kay, *The State Action Doctrine, the Public-Private Distinction, and the Independence of Constitutional Law*, 10 CONST. COMMENT. 329 (1993) (summarizing and commenting upon scholarly and judicial debate about the boundaries of the state action doctrine in the late twentieth century).

103. Isaiah Berlin, *Two Concepts of Liberty*, *in* ISAIAH BERLIN, FOUR ESSAYS ON LIBERTY 118, 127 (1969).

104. *See, e.g.*, Riley v. California, 134 S. Ct. 2473, 2494–95 (2014); Katz v. United States, 389 U.S. 347, 350 (1967).

105. *See, e.g.*, New Jersey v. T.L.O., 469 U.S. 325, 325 (1985).

106. *See, e.g.*, O'Connor v. Ortega, 480 U.S. 709, 709 (1987).

107. *See, e.g.*, Lawrence v. Texas, 539 U.S. 558, 558 (2003); Griswold v. Connecticut, 381 U.S. 479, 485 (1965).

108. *See* McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 342 (1995); Stanley v. Georgia, 394 U.S. 557, 559 (1969); *see also* RICHARDS, *supra* note 101; Daniel J. Solove, *The First Amendment as Criminal Procedure*, 82 N.Y.U. L. REV. 112 (2007).

109. *See, e.g.*, United States v. Katz, 389 U.S. 347, 350 (1967).

110. *See, e.g.*, *Griswold*, 381 U.S at 485 (1965).

111. *See* NASA v. Nelson, 562 U.S. 134, 138 (2010); Nixon v. Adm'r of Gen. Servs., 433 U.S. 425, 457 (1977); Whalen v. Roe, 429 U.S. 589, 599–600 (1977).

112. 429 U.S. at 605 (emphasis added).

113. For a sense of the wide range, see, e.g., Cooksey v. Boyer, 289 F.3d 513, 516 (8th Cir. 2002) (suggesting disclosures "must be either a shocking degradation or an egregious

So, sectoral statutes and torts cover narrowly defined behavior, and some additional constitutional proscriptions apply to government activity. But most private data-handling activities in the United States fall outside all these laws—generally including data mining by companies like Amazon or Google, files kept by local real estate brokers or bookstores, targeted advertising, most employee records, location tracking, shopper loyalty programs, and many more examples. Importantly for this Article, the massive data processing of Facebook (and other social media platforms) generally falls outside these rules too. Are the potential privacy issues raised by all these examples simply unregulated?

Well, no. In the absence of general-purpose omnibus privacy law like the E.U. Directive, consumer protection regulators such as the FTC and state attorneys general have moved in to fill the resulting vacuum.[114] This is the dominant consumer protection approach to privacy law in the United States.

Consumer protection law is tied to the inequitable nature of the underlying transaction, not to individual rights over personal data. The FTC imposes the most widely applicable privacy obligations on commercial entities in the United States. It does so by using its authority under Section 5 of its founding statute to police "unfair and deceptive acts or practices" in interstate commerce.[115] Attorneys general in individual states have also emerged as important enforcers of privacy law, using power granted under state consumer protection statutes that resemble the FTC's Section 5 authority.[116]

Consumer protection regulators like the FTC thus play a cleanup role in the system, regulating privacy where sectoral statutes do not. But even the FTC's Section 5 authority is limited not only by the substance of consumer protection, but also by activity that is nongovernmental, interstate, and commercial—and portions of specified industries are exempt from much FTC regulation, including some financial institutions, telecommunications carriers, and airlines.[117]

---

humiliation" to violate the constitutional right to privacy) (citing Alexander v. Peffer, 993 F.2d 1348, 1350 (8th Cir. 1993)); Am. Fed'n of Gov't Emps., AFL-CIO v. Dep't of Hous. & Urban Dev., 118 F.3d 786, 788 (D.C. Cir. 1997) (expressing "grave doubts as to the existence of a constitutional right of privacy in the nondisclosure of personal information"); J.P. v. DeSanti, 653 F.2d 1080, 1088 (6th Cir. 1981) (criticizing "courts [that] have uncritically picked up that part of *Whalen* pertaining to nondisclosure and have created a rule that the courts must balance a governmental intrusion on this 'right' of privacy against the government's interest in the intrusion"); United States v. Westinghouse Elec. Corp., 638 F.2d 570, 578 (3d Cir. 1980) (recognizing the right and articulating a multifactor test to apply it).

114. *See* Citron, *supra* note 15, at 3–4 (discussing the role of state attorneys general); Solove & Hartzog, *supra* note 15, at 585–86 (discussing the role of the FTC).

115. *See* 15 U.S.C. § 45(a) (2012). For informative accounts of the FTC's enforcement of privacy law through application of Section 5, see generally HOOFNAGLE, *supra* note 15; Solove & Hartzog, *supra* note 15.

116. *See* Citron, *supra* note 15, at 7–8.

117. *See* 15 U.S.C. § 45(a)(2) (2006) (listing exceptions from FTC authority); FTC v. AT&T Mobility, No. 15-16585, 2016 WL 4501685, at *3–5 (9th Cir. Aug. 29, 2016) (interpreting "common carrier" exception from FTC authority extremely broadly in a case outside of privacy law but applicable to all matters covered by Section 5, including privacy).

Where it applies, the FTC's Section 5 power is broad. As one court found in upholding the FTC's authority over privacy violations, unfair practices need not be otherwise unlawful, provided they meet the test for unfairness in the statute.[118] That test finds a practice unfair if it "[1] causes or is likely to cause substantial injury to consumers [2] which is not reasonably avoidable by consumers themselves and [3] [is] not outweighed by countervailing benefits to consumers or to competition."[119] In addition, Section 5 prohibits deceptive practices related to privacy—essentially any deviation in a company's actions from the material representations it has made about its data-handling practices. These "broken promises" could be found not only in a formal privacy policy, but also in, for example, marketing materials, help or support information such as FAQ's, or even the implications a reasonable person would draw from the interface on a website.[120]

The FTC has gradually developed working definitions of unfairness and deception by using responsive regulation techniques.[121] These evolving standards contrast with the detailed rules marking the boundaries of data protection law in Ireland. In its most basic form, the consumer protection model has long relied on concepts of "notice and choice" or "privacy control," requiring transparency about data-handling practices and giving individuals the ability to "opt out" by declining to proceed with a transaction.[122] This procedural focus—forcing disclosure and relying on market forces to embody consumers' privacy preferences—differs from the substantive requirements of a data protection model. It does not provide individuals with the broad rights of access or correction they have under the data protection model.[123] There is very little right to be forgotten under U.S. law either.[124]

---

118. *See* FTC v. Accusearch, Inc., 570 F.3d 1187, 1194 (10th Cir. 2009) (holding that Section 5 "enables the FTC to take action against unfair practices that have not yet been contemplated by more specific laws").

119. 15 U.S.C. § 45(n); *see* FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 244 (3d Cir. 2015) (tracing history of unfairness test).

120. *See In re* Snapchat, Inc., No. C-4501, 2014 WL 7495798, at *3–7 (Dec. 23, 2014) (charging a company with all these types of misrepresentations); *see also* Solove & Hartzog, *supra* note 15, at 628–33 (describing evolution of FTC interpretation of deceptive practices in the privacy context).

121. *See infra* Section III.B.

122. *See* Joel R. Reidenberg, *Restoring Americans' Privacy in Electronic Commerce*, 14 BERKELEY TECH. L.J. 771, 779 (1999); Paul M. Schwartz, *Internet Privacy and the State*, 32 CONN. L. REV. 815, 816 (2000).

123. A few extremely limited rights to examine personal data can be found in isolated parts of federal and state privacy law in the United States but nothing approaches Ireland's general right of access to personal data held by the private sector. *See, e.g.*, 15 U.S.C. § 1681g (2012) (providing consumers access to their own credit reports); 16 C.F.R. § 312.6 (2016) (providing right for parents to examine data collected from children under age 13 within scope of the statute); CAL. CIV. CODE § 1798.83 (West 2006) (providing right to be informed about disclosures of personal data to third parties).

124. In certain circumstances, California's new "Eraser Law" allows juveniles to withdraw information that they themselves have posted online. *See* CAL. BUS. & PROF. CODE § 22581 (West 2015). U.S. regulation of credit reports also prohibits the inclusion of certain personal data such as bankruptcies and tax liens after specified time periods. *See* 15 U.S.C.

In addition, unlike European and Irish laws, which provide legal redress to any affected individual—consistent with their understanding of data protection as a core human right—many U.S. statutes reserve enforcement power for administrative regulators alone. Only the FTC can enforce Section 5,[125] and individuals cannot bring private lawsuits under numerous sectoral data protection laws.[126] Some statutes do allow individual suits,[127] but even those opportunities are subject to considerable practical limitations, such as the need to prove particularized injury that confers standing to sue.[128] If this hurdle is passed, damages for individual claims may be small, which often means that class actions are the only viable mechanism for private action. Regulatory agencies have procedures for individuals to file complaints,[129] but unlike the ODPC and other E.U. data protection authorities, there is no obligation for U.S. agencies to act on these consumer grievances.

This Part's summary of the difference between Irish data protection law and U.S. consumer protection regulation "on the books" helps explain why conventional wisdom assumes European regulation is always much more demanding and protective of privacy than its American counterpart. The Article now turns to the use of responsive regulation techniques "on the ground" to show how enforcement choices can de-emphasize those distinctions and effectively promote privacy under either legal model.

II. RESPONSIVE REGULATION

A generation of administrative law scholars has debated numerous forms of "new governance"—many of them no longer all that new—that move beyond traditional command-and-control policymaking and enforcement to improve the

---

§ 1681c(a) (2012). But these are very narrow rights compared to those provided by the *Google Spain* case. *See* Case C-131/12, Google Spain v. Agencia Española de Protección de Datos, 2014 EUR-Lex CELEX LEXIS 62012CJ0131 (May 13, 2014).

125. *See* Sovern, *supra* note 18, at 1321–22, 1321 n.63.

126. *See, e.g.*, Gonzaga Univ. v. Doe, 536 U.S. 273, 274 (2002) (finding no private right of action under statute protecting privacy of student records); Acara v. Banks, 470 F.3d 569, 572 (5th Cir. 2006) (holding there is no private cause of action under HIPAA).

127. *See, e.g.*, Video Privacy Protection Act, 18 U.S.C. § 2710(c) (2012); Telephone Consumer Protection Act, 47 U.S.C. § 227(b)(3) (2012); Electronic Communications Privacy Act, 18 U.S.C. §2520 (2002). State consumer protection laws often permit individual suits. *See, e.g.*, CAL. CIV. CODE § 1780 (West 2010); VA. CODE ANN. § 59.1-204 (West 2016).

128. *See, e.g.*, Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1545 (2016) (requiring allegation of a privacy-related injury under FCRA to be both concrete and particularized in order to confer standing); Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1143 (2013) (finding allegations of electronic surveillance by intelligence agencies "too speculative to satisfy the well-established requirement that threatened injury must be certainly impending") (internal quotation omitted); *In re* iPhone Application Litig., 6 F. Supp. 3d 1004, 1012–15 (N.D. Cal. 2013) (finding lack of standing under California consumer protection statute).

129. *See How to File a Complaint with the Federal Trade Commission*, FED. TRADE COMMISSION (Jan. 19, 2012), https://www.ftc.gov/news-events/audio-video/video/how-file-complaint-federal-trade-commission; *Filing a HIPAA Complaint*, U.S DEP'T HEALTH & HUM. SERVS., http://www.hhs.gov/hipaa/filing-a-complaint/index.html (last visited Feb. 20, 2016).

effectiveness and legitimacy of regulation. These scholars also have sought to identify the ideal mixture of adversarial and cooperative approaches to maximize compliance with the law. In their landmark 1992 book, Ian Ayres and John Braithwaite captured the debate: "The crucial question has become: When to punish; when to persuade?"[130] While policymakers and legal scholars have increasingly embraced a wide range of creative and flexible approaches to traditional regulatory tasks in the intervening quarter century,[131] that question remains the crucial one today.

A. Coregulation: Theory and Reality

In privacy law, scholars and legislators most often have gravitated toward a particular flavor of new governance, sometimes called "coregulation," where agencies collaborate with industry groups or other third parties to develop detailed substantive rules.[132] These rules may then become enforceable law, frequently (though not always) subject to some approval or ratification by government regulators.[133] Coregulation and self-regulation can be partial or comprehensive and can entail various levels of government participation.[134] Whatever its structure, proponents of coregulation hope that active engagement with industry partners will make the resulting requirements more feasible and more widely accepted by regulated parties.

Several scholars have studied the possibility of privacy coregulation closely. In a series of articles, Dennis Hirsch has drawn on experiences of coregulation in environmental legislation[135] and in the data protection law of the

---

130. IAN AYRES & JOHN BRAITHWAITE, RESPONSIVE REGULATION 21 (1992).

131. *See* Orly Lobel, *The Renew Deal: The Fall of Regulation and the Rise of Governance in Contemporary Legal Thought*, 89 MINN. L. REV. 342, 344 (2004) (comprehensively reviewing "a paradigm shift from a regulatory to a governance model, signifying a collective intellectual and programmatic project for a new legal regime").

132. *See* AYRES & BRAITHWAITE, *supra* note 130, at 106; Jody Freeman, *Collaborative Governance in the Administrative State*, 45 UCLA L. REV. 1, 22 (1997) (using the term collaborative governance, instead of coregulation); Neil Gunningham & Joseph Rees, *Industry Self-Regulation: An Institutional Perspective*, 19 L. & POL'Y 363, 366 (1997); *cf.* CYNTHIA ESTLUND, REGOVERNING THE WORKPLACE: FROM SELF-REGULATION TO CO-REGULATION (2010) (applying related new governance concepts to labor and employment law).

133. *See* Ira S. Rubinstein, *Privacy and Regulatory Innovation: Moving Beyond Voluntary Codes*, 6 I/S: J. L. & POL'Y INFO. SOC'Y 355, 383 (2011) (describing government approval as necessary to ensure baseline regulatory objectives are met); *see also* BENNETT & RAAB, *supra* note 18, at 123–33 (describing different industry-generated self-regulatory instruments).

134. *See* NEIL GUNNINGHAM & PETER GRABOSKY, SMART REGULATION: DESIGNING ENVIRONMENTAL POLICY 50–55 (1998).

135. *See generally* Dennis D. Hirsch, *Protecting the Inner Environment: What Privacy Regulation Can Learn from Environmental Law*, 41 GA. L. REV. 1 (2006); Hirsch, *supra* note 15.

Netherlands[136] as possible models for data privacy rulemaking. Ira Rubinstein has developed a normative framework that identifies "six elements that are critical to the success of co-regulatory initiatives" in privacy law.[137]

Thus far, however, privacy coregulation in Ireland and in the United States has existed much more often as an idea than as reality. In theory, Ireland's Data Protection Act envisions reliance on industry-created codes of practice.[138] In reality, there are few examples. There is a code concerning data breach notification, but the ODPC treats it as a statement of best practices and not as a source of authoritative legal obligations or defenses.[139] Otherwise almost all codes of practice approved by ODPC focus on public-sector entities.[140] The GDPR contains similar rules for coregulation through codes of conduct and certification marks, but it is unclear whether implementation of this approach will be any more common in Ireland than it is today.[141]

There is even less demonstrated adoption of coregulation in U.S. privacy law. In one instance, HIPAA mandated that data security regulations governing healthcare providers and insurers must be developed with significant input from industry players through a preexisting advisory board.[142] David Thaw examined this process and found several fairly unusual attributes that, he argues, made it a coregulation success story.[143] Otherwise, coregulation has been a cornerstone of *proposed* legislation in the United States, including the Obama Administration's

---

136. *See generally* 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 (2014).

137. Rubinstein, *supra* note 133, at 380. The elements are: "efficiency, openness and transparency, completeness, strategies to address free rider problems, oversight and enforcement, and use of second-generation design features." *Id*.

138. Irish Data Protection Act, *supra* note 51, § 14(a)(2).
(instructing Commissioner to "encourage trade associations and other bodies representing categories of data controllers to prepare codes of practice to be complied with by those categories in dealing with personal data").

139. *See* CAREY, *supra* note 56, at 71.

140. *See id.* at 161; DATA PROTECTION COMM'R, *Annual Report of the Data Protection Commissioner of Ireland 2014*, at 11, https://www.dataprotection.ie/docimages/documents/Annual%20Report%202014.pdf. [hereinafter 2014 Annual Report]. For an example, see PERS. INJURY ASSESSMENT BD., *Data Protection Code of Practice* (Jan. 9, 2008), http://www.injuriesboard.ie/eng/resources/Data_Protection_Code_of_Practice/Data_Protection_Code_of_Practice.pdf.

141. GDPR, *supra* note 13, at arts. 40–43.

142. *See* 42 U.S.C. §§ 1320d-1–d-2(2012).

143. *See* David Thaw, *Enlightened Regulatory Capture*, 89 WASH. L. REV. 329, 353–62 (2014). Thaw identifies the historical roots of the advisory committee involved (an elite body of top professionals that has existed since the 1950s), the collective good of cybersecurity in a closed industry, and the ability of the federal Department of Health and Human Services to write its own rules if these experts could not agree. *Id.* at 364–67. These features would be difficult to recreate in a more contentious and open-ended issue area (like most privacy issues) and without a preexisting elite advisory board.

marquee privacy initiative[144] and numerous bills sponsored by members of Congress from both parties.[145] None of these became law.

Coregulation may be a promising mechanism for the future development of privacy law, but there are significant limitations that would make it difficult to apply broadly in a system like that in the United States or Ireland. First, where it exists, coregulation often depends on unique historical features. For example, as Hirsch explained in his comprehensive study, Dutch privacy coregulation depends on the longstanding and widespread tradition of cooperative regulation in the Netherlands known as the "polder model," named for areas of land below sea level that were reclaimed through massive cooperative effort on the country's famed dikes and pumps.[146] Second, most proposals for coregulation—including those introduced in Washington, D.C.—contemplate an elaborate multilateral consultation process seeking broad consensus about privacy law.[147] While stakeholder involvement would confer more legitimacy on coregulation efforts, it would also make true consensus much more difficult and expensive to accomplish.[148] For example, the effort to develop a "do not track" protocol for websites[149] foundered because industry representatives and privacy advocates could never reach consensus on fundamental issues after years of acrimonious effort, and the initiative's final product was extremely limited.[150]

---

144. *See* Consumer Privacy Bill of Rights Act of 2015 17–20 (Discussion Draft), https://www.whitehouse.gov/sites/default/files/omb/legislative/letters/cpbr-act-of-2015-discussion-draft.pdf (proposing safe harbors from liability for data processing conducted in compliance with industry-developed codes of conduct).

145. *See* Best Practices Act, H.R. 611, 112th Cong. § 401 (2011); Consumer Privacy Protection Act of 2011, H.R. 1528, 112th Cong. § 9 (2011); Commercial Privacy Bill of Rights Act of 2011, S. 799, 112th Cong. § 501 (2011).

146. *See* Hirsch, *supra* note 136, at 123–25. There is a vast academic and journalistic literature on the polder model. *See, e.g.*, LEI DELSEN, EXIT POLDER MODEL?: SOCIOECONOMIC CHANGES IN THE NETHERLANDS (2002); Yda Schreuder, *The Polder Model in Dutch Economic and Environmental Planning*, 21 BULL. SCI. TECH. SOC. 237 (August 2001); *Same Old Dutch: Is the Polder Model Back?*, ECONOMIST (Nov. 3, 2012), http://www.economist.com/news/europe/21565661-polder-model-back-same-old-dutch.

147. For a powerful normative argument about the importance of such broad participation, see Freeman, *supra* note 132, at 77–82; *see also* Rubinstein, *supra* note 133, at 421.

148. *See* Mark Seidenfeld, *Empowering Stakeholders: Limits on Collaboration as the Basis for Flexible Regulation*, 41 WM. & MARY L. REV. 411, 450 (2000).

149. *Tracking Protection Working Group*, WORLD WIDE WEB CONSORTIUM, http://www.w3.org/2011/tracking-protection/ (last visited July 8, 2014).

150. *See* Dawn Chmielewski, *How 'Do Not Track' Ended Up Going Nowhere*, RE/CODE (Jan. 4, 2016), http://recode.net/2016/01/04/how-do-not-track-ended-up-going-nowhere; Kate Kaye, *Do Not Track Is Finally Coming, But Not as Originally Planned*, ADVERTISING AGE (July 17, 2015), http://adage.com/article/privacy-and-regulation/track-finally-coming-planned/299536/. I attended the first workshop to explore a do-not-track effort in April 2011 at Princeton University, *see W3C Workshop on Web Tracking and User Privacy*, WORLD WIDE WEB CONSORTIUM, https://www.w3.org/2011/track-privacy/ (last visited Feb. 15, 2016), and decided at once that the effort was doomed—but I was sorry to be proven correct. My interest in the concept of user agents communicating binding privacy

B. The Responsive Regulation Model

All the focus on coregulation bypasses another approach that is already in use: responsive regulation. While coregulation focuses primarily on the content of rules, responsive regulation is concerned with the method of enforcing the rules, regardless of their substance. And while coregulation presupposes many interested parties achieving broad consensus, responsive regulation simply influences the behavior of a regulator toward all regulated entities. Even when rules have been written largely or entirely through traditional governmental processes, they can be applied with an eye toward collaboration. Unlike coregulation, which rarely has been implemented to govern privacy, responsive regulation of privacy already exists in fact. Indeed, it dominates enforcement of privacy law in both Ireland and the United States.

The model of responsive regulation strongly associated with Ayres and Braithwaite is typically illustrated as a pyramid.[151] Tactics of dialogue and persuasion lie at the broad base of the pyramid; agencies should use these first and most frequently.[152] Such informal methods often spur regulated entities to improve their practices without any official action at all. The government can rely heavily on this strategy of advice, exhortation, and industry cooperation, turning to penalties only when these methods fail.[153] At the next level up the pyramid, methods may be more formal but still not directly punitive. A warning letter or a public rebuke might get the attention of a company's leadership. Even an announcement that a practice will be investigated can have the desired effect of fixing the problem. The classic pyramid then moves up through civil penalties to criminal ones. At the apex of the pyramid are "nuclear" weapons such as the revocation of a company's license to operate.[154]

Responsive regulation works in a wide range of industries.[155] Generally speaking, agencies use responsive regulation to relate to businesses under their

---

preferences goes all the way back to my first piece of published legal scholarship. *See* William McGeveran, Note, *Programmed Privacy Promises: P3P and Web Privacy Law*, 76 N.Y.U. L. REV. 1812 (2001). In the interminable discussions surrounding proposals for both do-not-track and P3P, stakeholders disagreed on fundamental binary decision points, and there was no way to move past those disputes without a polder model, Hirsch, *supra* note 136, at 123–24, or the types of institutional structures identified by Thaw, see *supra* note 143, at 371.

151. *See* AYRES & BRAITHWAITE, *supra* note 130, at 35–40; JOHN BRAITHWAITE, RESTORATIVE JUSTICE AND RESPONSIVE REGULATION 30–34 (2002).

152. AYRES & BRAITHWAITE, *supra* note 130, at 35.

153. *Id*. at 35–48.

154. *Id*.; *see also* BRAITHWAITE, *supra* note 151, at 30–34 (summarizing the pyramid approach); GUNNINGHAM & GRABOSKY, *supra* note 134, at 396–97.

155. *See, e.g.*, Kenneth W. Abbott et al., *Soft Law Oversight Mechanisms for Nanotechnology*, 52 JURIMETRICS J. 279, 286–96 (2012) (identifying 11 "soft law" mechanisms for governance of nanotechnology); Stuart Hogarth et. al., *Closing the Gaps—Enhancing the Regulation of Genetic Tests Using Responsive Regulation*, 62 FOOD & DRUG L.J. 831, 839–47 (2007) (applying disclosure and guidance strategies to the regulation of genetic testing); Daniel Schwarcz, *Redesigning Consumer Dispute Resolution: A Case Study of the British and American Approaches to Insurance Claims Conflict*, 83 TUL. L. REV. 735,

authority more as partners than as antagonists. At the base of the pyramid, they rely upon such "soft law" techniques as education, guidance, dialogue, advice, and transparency prior to using adversarial methods.[156] Responsive regulatory regimes might resolve individual controversies through consultation and dispute resolution with companies and the individuals affected by their practices.[157] While the underlying possibility of fines or other legal sanctions surely influences the use of all of these methods and their success, responsive regulation keeps them in the background. If they eventually impose punishments, regulators do so primarily to remedy shortcomings, not to seek retribution. As one well-known article explains, "regulators begin by assuming virtue (to which they should respond by offering cooperation), but when their expectations are disappointed, they respond with progressively punitive and deterrent-oriented strategies until the regulatee conforms."[158]

Relying on the implied threat of punishment to get results without actually imposing the penalty is a very old idea. Parents have probably relied on this method since Eve gave birth to Cain and Abel. Sun Tzu described it as a military tactic.[159] Perhaps its most famous invocation in modern times came from Theodore Roosevelt in a speech at the Minnesota State Fair, where he advocated that U.S. diplomacy should "speak softly but carry a big stick."[160] When he was an early chair of the Securities and Exchange Commission in the 1930s, the future Supreme Court Justice William O. Douglas explicitly applied the same thinking to regulatory style, arguing that government agencies like his ought to "keep the shotgun, so to speak, behind the door, loaded, well oiled, cleaned, ready for use but with the hope it would never have to be used."[161]

Ayres and Braithwaite call this the "benign big gun" model of enforcement.[162] Perhaps unlike Sun Tzu and Roosevelt's geopolitical methods, however, responsive regulation does not work well if the only penalties a regulator can exact resemble all-out war. When the only possible punishments are so serious that imposing them would be politically perilous, the threat to use them loses

---

770–79 (2009) (describing the well-established conciliation process for insurance disputes in the United Kingdom).

156. GUNNINGHAM & GRABOSKY, *supra* note 134, at 60–69 (reviewing educational and information-forcing regulatory instruments); *see* BENNETT & RAAB, *supra* note 18, at 111–12 (discussing educational efforts undertaken by data protection regulators in multiple jurisdictions); HOOFNAGLE, *supra* note 15, at 100 (stating that "the FTC's primary tactic in privacy is an information-forcing one, namely the workshop").

157. *See, e.g.*, Schwarcz, *supra* note 155, at 750–55.

158. Neil Gunningham & Darren Sinclair, *Integrative Regulation: A Principle-Based Approach to Environmental Policy*, 24 LAW & SOC. INQUIRY 853, 864 (1999).

159. SUN TZU, THE ART OF WAR 77 (Samuel Griffith trans., 1963) ("To subdue the enemy without fighting is the acme of skill.").

160. Ben Welter, *Sept. 3, 1901: Roosevelt 'Big Stick' Speech at State Fair*, STAR TRIB. (Minn.) (Sept. 2, 2014, 6:08 PM), http://www.startribune.com/sept-3-1901-roosevelt-big-stick-speech-at-state-fair/273586721/.

161. WILLIAM O. DOUGLAS, DEMOCRACY AND FINANCE 82 (1940).

162. AYRES & BRAITHWAITE, *supra* note 130, at 38–41.

credibility.[163] Rather, regulators should have a wide range of options available, from small consequences to very large ones, but keep them in the background. Regulators can then use the specter of penalties for leverage when operating informally at the base of the pyramid.[164] At the middle levels of the pyramid, some of the agencies' actions might impose consequences, but part of their power remains in the possibility of more severe punishments. The largest penalties should be Douglas's metaphorical oiled shotguns, kept the furthest behind the door—but the mere knowledge of their existence can influence compliance by regulated entities.[165]

Responsive regulation is a general model, not a precise blueprint. The specific nature of the actions at every level of the pyramid will differ depending on factors like the nature of the regulated industry, the harm caused by infractions, and the powers of the regulator. Moreover, no single regulatory formula is ideal for every situation.[166] In fact, supporters of responsive regulation and other cooperative enforcement strategies usually emphasize that most circumstances call for a well-considered mixture of strategies, including some more traditional ones.[167] Bennett and Raab recognized this over a decade ago when they summed up the varied functions played by data protection authorities: "Commissioners act, variously, as ombudsmen, auditors, consultants, educators, negotiators, policy advisers, and enforcers. Not every role is played with equal weight by every commissioner. Nor are these functions the exclusive responsibility of the data protection agency . . . ."[168] Billy Hawkes, Ireland's former Data Protection Commissioner, summarized his tasks under Irish law in similar terms: an "enforcer role," an "ombudsman role," an "educational role," and a "transparency role."[169] As elaborated in the next Section and in Parts III and IV, Ireland and the United States both use the regulatory pyramid approach to combine these roles in their privacy enforcement.

C. Responsive Privacy Regulation

Several features of privacy compliance make it particularly well-suited to responsive regulation. First, responsive regulation works most effectively when regulated parties are otherwise motivated to do their best to comply with the law. This makes the starting assumption of good faith more likely to be accurate. Naturally, many companies seeking to monetize the value of customer data will view

---

163. *See id*. at 45–46.

164. *Id*. at 38.

165. *See id*. at 47–48. As Greenleaf notes, however, these penalties must be serious enough to command the attention of regulated entities. *See* Greenleaf, *supra* note 19, at 258. *See generally* Hazel Grant & Hannah Crowther, *How Effective Are Fines in Enforcing Privacy?*, *in* ENFORCING PRIVACY, *supra* note 15, at 287.

166. *See id*. at 101; GUNNINGHAM & GRABOSKY, *supra* note 134, at 388 (discussing how a variety of approaches are best used together).

167. *See* GUNNINGHAM & GRABOSKY, *supra* note 134, at 388–90 (concluding that "regulatory pluralism" is necessary for optimal effectiveness).

168. BENNETT & RAAB, *supra* note 18, at 109; *see also id.* at 109–114 (expanding on the roles).

169. Billy Hawkes, *The Irish DPA and Its Approach to Data Protection*, *in* ENFORCING PRIVACY, *supra* note 15, at 441, 442–43.

privacy regulation differently than the strongest privacy advocates. Nonetheless, few companies see privacy as an area where they strive to get away with as much as legally possible. Companies and their investors know that their privacy and security practices influence brand value, customer trust, and ultimately, profitability.[170] Customer-facing companies of all types and sizes develop detailed voluntary privacy policies and make them public.[171]

These efforts to observe privacy limits that extend beyond the legally required minimum contrast with areas where the regulated entity strives to go as far as possible without being penalized. Tax enforcement might be such an example: most businesses would regard paying even a penny more tax than legally necessary to be a blunder.[172] Privacy is not an area where the dominant ethos encourages companies to push every boundary so long as they have a colorable legal argument to defend their behavior. Regulators may still determine that policies or practices are inadequate, but at a minimum, most businesses want to portray themselves, and to *perceive* themselves, as safeguarding the privacy of their customers.

At a minimum, companies' inclination to embrace best practices helps make regulators' collaborative efforts effective. But responsive regulation may actually encourage those motivations. In their empirical study interviewing corporate privacy officials in five countries, Bamberger and Mulligan found that their interview subjects in the United States and Germany, the countries with the more open-textured rules, understood privacy and data protection obligations in terms of risk management and the formulation of company policies that match consumer expectations, not as a function of compliance with settled law.[173]

---

170. *See* Colin Scott, *Reflexive Governance, Meta-Regulation, and Corporate Social Responsibility: The 'Heineken Effect'*, in PERSPECTIVES ON CORPORATE SOCIAL RESPONSIBILITY 170, 177–82 (Nina Boeger et al. eds., 2008); Ronen Shamir, *Capitalism, Governance, and Authority: The Case of Corporate Social Responsibility*, 6 ANN. REV. L. & SOC. SCI. 531, 540–44 (2010). For example, both Apple and the FBI concluded that the company's public stand in favor of customer privacy during their highly publicized dispute over iPhone encryption enhanced Apple's brand. *See* Klint Finley, *Apple's Noble Stand Against the FBI Is Also Great Business*, WIRED (Feb. 17, 2016), http://www.wired.com/2016/02/apples-noble-stand-against-the-fbi-is-also-great-business/; Will Oremus, *Irate DOJ Dismisses Apple's Fight with the FBI as a 'Brand Marketing Strategy,'* SLATE (Feb. 19, 2016), http://www.slate.com/blogs/future_tense/2016/02/19/department_of_justice_motion_mocks_apple_s_fbi_fight_as_a_brand_marketing.html.

171. For the most part, companies post detailed privacy policies voluntarily. *See* MCGEVERAN, *supra* note 23, at 166–67. California law requires most companies to post privacy policies on their websites. CAL. BUS. & PROF. CODE § 22575 (West 2014). However, that law does not mandate the contents or level of detail in these policies, nor does it require them to cover data collected through mechanisms other than the website.

172. Even in this realm, responsive regulation is on the rise. *See* Valerie Braithwaite et al., *Taxation Threat, Motivational Postures, and Responsive Regulation*, 29 LAW & POL'Y 137 *passim* (2007); Sagit Leviner, *A New Era of Tax Enforcement: From "Big Stick" to Responsive Regulation*, 42 U. MICH. J.L. REFORM 381, 385–86 (2009).

173. BAMBERGER & MULLIGAN, *supra* note 16, at 59–104. Their findings are consistent with my own interactions with U.S. corporate privacy officials.

Corporate officials in Spain and France, where authorities have used responsive techniques less readily, had an attitude more oriented toward technical compliance.[174] This contrast supports the notion that friendlier regulatory styles can actually catalyze corporate social responsibility and the formation of privacy-protective norms, motivated not only by concern about the risk of legal penalties but also by other economic and social incentives.[175]

Second, rapid technological change increases the benefits of responsive regulation. Scholars commonly point out the challenge of keeping the law current with developing digital architecture, and with social and business adaptations to that technology. It is expensive to keep command-and-control regulations up to date in those circumstances.[176] A costly game of regulatory whack-a-mole ensues, as the rules adjust to new technology or practices, which then adjust to evade the rules. Responsive regulation establishes continuing dialogue rather than fixed dictates. That makes it a particularly strong response to situations where lawmakers have difficulty staying abreast of rapid technological change.[177]

By using responsive regulation based on broader principles, regulators can secure compliance even as the details of technology change. At the same time, the resulting flexibility enables continuous change and improvement of interfaces and business methods—indeed, not just enables but encourages it. Rather than giving up on the possibility of controlling the inexorable evolution of technology, responsive regulation allows agencies to respond to those changes and ameliorate privacy impacts without throttling productive innovation.[178]

There are, of course, dangers in responsive regulation as well. It can be used to cloak inaction and laxity. Some scholars argue that responsive regulation increases the likelihood of harmful agency capture or overestimates the rational and moral behavior of corporations.[179] Furthermore, it can be perceived by the public as a charade, undermining confidence in the seriousness of enforcement of the law. In addition, if a regulator concentrates too much on private resolution of individual

---

174. *Id*. at 105–143.

175. *Id*. at 219–37; *cf*. BENNETT & RAAB, *supra* note 18, at 133–34 (discussing these factors in the context of self-regulation).

176. *See* AYRES & BRAITHWAITE, *supra* note 130, at 26.

177. *Id*.

178. The Facebook case study considered in Part IV includes an example of innovation that could have been throttled by unduly strong and potentially premature command-and-control restrictions. *See infra* notes 290–93 and accompanying text (discussing controversy surrounding Facebook's introduction of its News Feed feature and subsequent widespread acceptance of its benefits).

179. *See, e.g.*, Sara Singleton, *Co- Operation or Capture? The Paradox of Co-Management and Community Participation in Natural Resource Management and Environmental Policy-Making*, 9 ENVTL. POL., Summer 2000, at 1, http://dx.doi.org/10.1080/09644010008414522 (analyzing capture in locally devolved co-management of natural resources); Steve Tombs, *Understanding Regulation?*, 11 SOC. & LEGAL STUDS. 113, 126–28 (2002) (book review) (criticizing new governance scholars for failing to account for power dynamics and for assuming too much moral and socially responsible behavior by corporate entities).

complaints and advice, it may fail "to make law general" in a way that shapes other parties' behavior effectively.[180] Finally, agencies that rely on responsive regulation without "broader political and cultural support for the regulator's view of the law" may find themselves forced either to revert to old-fashioned punitive enforcement or to capitulate and relax enforcement entirely.[181]

All that said, every approach to regulation includes risks. And there are considerable advantages to responsive regulatory techniques. They generally are more flexible and cost-effective than the alternatives.[182] They also create incentives for entities to promote internal compliance and best practices, especially if they know that the regulator will look more kindly on alleged lapses where sincere efforts have been made to embrace best practices.[183] Most of all, in an area like privacy regulation, where fixed rules are difficult to articulate, collaboration with organizations holding personal data may be the only realistic way to protect individual interests.

Part V will return to some lessons about improving responsive privacy regulation to avoid its potential pitfalls. If used wisely, responsive regulation techniques can ensure compliance with privacy laws effectively. Part III looks at the overall implementation of responsive regulation in Ireland and the United States, and Part IV then turns to the specific example of the Facebook case study.

III. RESPONSIVE PRIVACY REGULATION IN IRELAND AND THE U.S.

This Part looks at the regulatory strategy adopted by the ODPC in Section A and by the main U.S. regulator, the FTC, in Section B. While doing so, it also returns to the two questions that opened this Article. First, how does the similar regulatory strategy in these two countries bridge gaps between the differing legal requirements described in Part I? Second, how does the responsive regulatory approach they have chosen actually work? This Part and the Facebook case study in Part IV pursue answers to those questions.

We will see that the two countries' convergent regulatory styles promote comparable best practices in data handling on both sides of the Atlantic. Francesca Bignami has traced a convergence of data protection enforcement in Britain, France, Germany, and Italy toward "cooperative legalism" that uses "the threat of inspections and sanctions to induce market[] actors to take privacy standards

---

180. Susan S. Silbey, *The Consequences of Responsive Regulation*, *in* ENFORCING REGULATION 147, 161–64 (Keith Hawkins & John M. Thomas eds., 1984).

181. Christine Parker, *The 'Compliance' Trap: The Moral Message in Responsive Regulatory Enforcement*, 40 LAW & SOC'Y REV. 591, 611–13 (2006).

182. *See* BRAITHWAITE, *supra* note 151, at 31–34.

183. *See, e.g.*, BAMBERGER & MULLIGAN, *supra* note 16, at 69–70 (discussing reactions to the FTC's enforcement strategies); *cf.* Heather K. Gerken, *A Third Way for the Voting Rights Act: Section 5 and the Opt-In Approach*, 106 COLUM. L. REV. 708, 729–30 (2006) (applying a similar concept to local government compliance with the Voting Rights Act).

seriously."[184] Bamberger and Mulligan have found that regulatory behavior helped explain similarities in corporate behavior related to privacy in the U.S. and Germany.[185] So it is with the United States and Ireland. Shortly before he left office in 2014, Ireland's former Data Protection Commissioner, Billy Hawkes, drew the same conclusion in a speech:

> As Ireland is a welcoming home for many US multinationals, we have a particular interest in aiming for interoperability between EU and US models of privacy protection. Privacy is a shared value, as is evident from the broad agreement on privacy principles. . . .Recently attending a conference in the US, I was struck by the fact that the good practice advice from panels was not very different from what you would hear at a European event.[186]

As for its effectiveness, the remedial actions required by the ODPC under Irish law seem generally to satisfy the aggrieved citizens who lodge complaints.[187] The FTC's consent decrees typically impose 20-year privacy compliance programs and continued FTC oversight on companies.[188] Those facts provide a partial answer to be taken up again in Part IV.

A. Ireland: The ODPC

Ireland is a very small country with a comparatively prosperous economy. A population of just over 4.5 million makes it the smallest of the long-term (Cold War era) E.U. members except for Luxembourg.[189] Traditionally, Ireland was also considered among the "Poor Four" of those E.U. states along with Portugal, Spain, and Greece.[190] Then the economy, and especially the real estate market, overheated

---

184. Bignami, *supra* note 15, at 460. Bennett noted indications of convergence in the data protection law of Europe and the United States back in 1992. BENNETT, *supra* note 18, at 95–115.

185. *See* BAMBERGER & MULLIGAN, *supra* note 16, at 219–25.

186. Billy Hawkes, Data Protection Comm'r, Address at the Institute of International and European Affairs: Data Protection – the State, Technology and other Challenges 5 (July 21, 2014).

187. *See infra* notes 214–18 and accompanying text.

188. *See infra* notes 249–57 and accompanying text.

189. Ireland joined the European Community, the precursor to the E.U., in 1973 along with Denmark and the United Kingdom; these were the first nations to join since the "Inner Six" founders began forming cooperative European bodies in the 1950s. A number of smaller countries joined in 2004 and later during the significant enlargement of the E.U. after the end of the Cold War. *See European Union*, ENCYCLOPEDIA.COM (2009), http://www.encyclopedia.com/social-sciences-and-law/political-science-and-government/international-organizations/european-union (last visited Oct. 9, 2016). Ireland also has a smaller population than half the states in the United States: according to the U.S. Census estimates for July 2015, Louisiana is ranked 25th among states with a population of 4.6 million; while the 26th state, Kentucky, has a population of 4.4 million people. *Louisiana*, U.S. CENSUS BUREAU, http://www.census.gov/quickfacts/table/PST045215/22 (last visited Sept. 19, 2016).

190. *See* Alan Riding, *Europe's 'Poor 4' Demand More Aid*, N.Y. TIMES (Dec. 5, 1991), http://www.nytimes.com/1991/12/05/world/europe-s-poor-4-demand-more-aid.html.

during the "Celtic Tiger" boom of the 1990s and early 2000s, leading to a devastating crash. Along with the other "Poor Four," Ireland required an E.U. bailout, but it was the first of the four to exit the bailout[191] and is now emerging from the worst of the financial crisis.[192] In 2015, according to the World Bank, Ireland's per capita GDP (adjusted for purchasing power parity) was an enviable $54,654, just a tiny bit less than the per capita rate in the United States and higher than that of every E.U. member state except Luxembourg.[193] Housing prices and long-term unemployment remain serious problems, but Ireland has secured a place as a tiny sibling among the first rank of global industrial powers.

Much of the previous boom and the current recovery derive from Ireland's remarkable success in attracting foreign investment of all kinds, particularly within the technology sectors. *Forbes Magazine* routinely ranks Ireland near the top of its annual list of the world's most pro-business countries.[194] And some of the best-known firms in the information industry—including not only Facebook, but also Google, Intel, Apple, Twitter, LinkedIn, PayPal, and eBay—have established large operations in Ireland.[195] These Irish outposts manage American companies' activities in many countries: some cover all of Europe, some add the Middle East and Africa, and others are responsible for data collected from the entire world outside the United States (or, as in Facebook's case, outside the United States and

191. Henry McDonald, *Ireland Becomes First Country to Exit Eurozone Bailout Programme*, GUARDIAN (Dec. 13, 2013), https://www.theguardian.com/business/2013/dec/13/ireland-first-country-exit-eurozone-bailout.

192. *See* Tara Cunningham, *Is the Celtic Tiger Really Ready To Roar Again?*, TELEGRAPH (Nov. 28, 2015), http://www.telegraph.co.uk/finance/economics/12022109/Is-the-Celtic-Tiger-really-ready-to-roar-again.html.

193. *See GDP Per Capita, PPP (Current International $)*, WORLD BANK, http://data.worldbank.org/indicator/NY.GDP.PCAP.PP.CD (last visited Aug. 16, 2016). Purchasing power parity (PPP) adjustments to GDP figures are a widely accepted method to equalize currency calculations so that comparisons between countries are not distorted by fluctuating currency exchange rates. *See Frequently Asked Questions*, *Purchasing Power Parities*, OECD http://www.oecd.org/std/prices-ppp/purchasingpowerparities-frequentlyaskedquestionsfaqs.htm (last visited Aug. 16, 2016).

194. Ireland ranked first in the world on the 2013 list. Kurt Badenhausen, *Ireland Heads Forbes' List of the Best Countries for Business*, FORBES (Dec. 4, 2013), http://www.forbes.com/sites/kurtbadenhausen/2013/12/04/ireland-heads-forbes-list-of-the-best-countries-for-business/. It was fourth in the most recent ranking, behind Denmark, New Zealand, and Norway. Kurt Badenhausen, *The Best Countries for Business 2015*, FORBES (Dec. 16, 2015), www.forbes.com/sites/kurtbadenhausen/2015/12/16/the-best-countries-for-business-2015.

195. *See* Breathnach, *supra* note 10; Burrell, *supra* note 2.

Canada).[196] As of 2014, this rapidly growing information technology sector accounted for 40% of Irish exports.[197]

There are many reasons why so many high-tech multinationals have set up shop in Ireland, most notably Europe's lowest corporate tax rate and controversial rules concerning tax residency and transfer pricing that enable companies to further reduce their tax liability.[198] Other attractions for U.S. tech companies include a very well-educated workforce, low labor costs due to stubborn unemployment rates, and universal English.[199] There is reason to believe that regulatory policy further contributes to the appeal. Facebook privacy executives have indicated that the country's regulatory environment was one of several reasons the company chose to base such a large operation in Ireland.[200] Whatever their original motivation for setting up second homes in Ireland, technology companies are now a substantial presence in Ireland's still-fragile economy, making cooperative data protection enforcement a high priority for the government there.

Ireland's original 1988 Data Protection Act established the position of Data Protection Commissioner and empowered that official to enforce the Data Protection Act across all industries, including the government and non-profit sectors as well as businesses of every type.[201] While there was little reason at the time to expect the

---

196. Twitter, for example, implemented this shift in 2015, changing its terms of service so that all non-U.S. users have a legal relationship with Twitter's Irish subsidiary rather than its U.S.-based parent company. *See* Mark Paul, *Ireland to Become Privacy Regulator for 300m Twitter Users*, IRISH TIMES (Apr. 17, 2015), http://www.irishtimes.com/business/technology/ireland-to-become-privacy-regulator-for-300m-twitter-users-1.2180137. Facebook has long used the same technique for all users outside the United States and Canada. *See* DATA PROT. COMM'R, *Report of Audit: Facebook Ireland Ltd.* 3 (Dec. 21, 2011), http://www.dataprotection.ie/docs/Facebook-Ireland-Audit-Report-December-2011/1187.htm [hereinafter ODPC Facebook Audit].

197. Burrell, *supra* note 2.

198. James Kanter & Landon Thomas Jr., *Tax Deals Are Target of Inquiry in Europe*, N.Y. TIMES (June 12, 2014), http://www.nytimes.com/2014/06/12/business/international/eu-to-investigate-countries-business-tax-breaks.html. The IRS has disputed Facebook's valuation of assets transferred to Ireland and is now pursuing the company for an alleged tax deficiency of between 3 and 5 billion dollars, plus interest and penalties, in relation to its Irish operations. *See* Kartikay Mehrotra, *Facebook Tax Bill Over Ireland Move Could Cost $5 Billion*, BLOOMBERG (July 28, 2016), http://www.bloomberg.com/news/articles/2016-07-28/facebook-gets-3-5-billion-irs-tax-notice-over-ireland-move.

199. Kurt Badenhausen, *Ireland Heads Forbes' List of the Best Countries for Businesses*, FORBES (Dec. 4, 2014, 9:58 AM), http://www.forbes.com/sites/kurtbadenhausen/2013/12/04/ireland-heads-forbes-list-of-the-best-countries-for-business/#13d7ed541e6a. Also, it must be said: excellent beer and music, friendly people, and beautiful scenery.

200. Karin Lillington, *Ireland's Regulatory Reputation Encouraged Facebook HQ*, IRISH TIMES (Jul. 9, 2015), http://www.irishtimes.com/business/technology/ireland-s-regulatory-reputation-encouraged-facebook-hq-1.2279283 ("Facebook set up its operations in Ireland in part because it felt the regulatory environment 'was seen as a good high standard' internationally.").

201. Irish Data Protection Act 1988, *supra* note 50, § 9.

ODPC to play a pivotal role in regulating the data-handling practices of so many high-tech multinationals from around the globe, the structure laid out in that 1988 statute remains in place. The underlying law will change when the GDPR becomes effective in 2018, but primary regulatory authority will remain with the ODPC (subject to some new pan-European procedures, discussed below).[202]

The Act's text directly promotes responsive regulation. One of its key provisions allows individuals to file complaints with the ODPC alleging violations of data protection law, although the ODPC is also free to pursue actions on its own initiative.[203] The Act decrees that the ODPC "shall" investigate each complaint received unless it is "frivolous or vexatious."[204] The ODPC is obliged to seek an "amicable resolution" of such complaints first, and to move to more formal processes if this is not possible "within a reasonable time."[205] Those dissatisfied with the outcome may appeal to the Irish courts.[206] From there, cases may be referred to the E.U. judicial system. Schrems, the Austrian privacy activist, took this opportunity when displeased with the ODPC's response to his complaint about Facebook transferring data to the U.S. under the Safe Harbor Agreement; he appealed to the Irish High Court, and his case went from there to the Court of Justice of the European Union, the highest in the E.U.[207] In addition to striking down Safe Harbor, the Court of Justice held that national data protection authorities are *obliged* to exercise their investigatory and enforcement powers in response to citizen complaints.[208]

This architecture encourages the use of the responsible regulation pyramid. The statutory text requires the use of consultation first, and allows a move toward more punitive measures if (and only if) those fail.[209] Annual reports produced by the ODPC demonstrate how these statutory instructions are applied in practice. The reports, among other things, provide statistics about the complaints received that year and summarize "case studies" of the actions taken and conclusions reached.[210]

The statistics indicate that intervention, negotiation, and settlement are a great deal more common than adversarial processes at the ODPC. According to its annual reports, the ODPC has received between 900 and 1,350 complaints per year

---

202. *See infra* notes 403–06 and accompanying text.

203. Irish Data Protection Act 1988, *supra* note 50, § 10(1A); *see Complaint Form*, DATA PROTECTION COMMISSIONER, https://www.dataprotection.ie/raise-a-concern/ (last visited June 19, 2016).

204. Irish Data Protection Act 1988, *supra* note 50, § 10(b); *see also* CAREY, *supra* note 56, at 157 (explaining complaint procedure).

205. Irish Data Protection Act 1988, *supra* note 50, § 10(a)(ii).

206. *Id.; see also infra* Section V.A.3.

207. *See infra* notes 389–91 and accompanying text.

208. *See* Schrems v. Data Prot. Comm'r, 2015 EUR-Lex CELEX LEXIS 62014CJ0362 (Oct. 6, 2015).

209. Irish Data Protection Act, *supra* note 51, § 10(b)(ii).

210. For annual reports dating back to 1997, see *Annual Reports*, DATA PROTECTION COMMISSIONER https://www.dataprotection.ie/ViewDoc.asp?fn=/documents/annualreports/ARHome.htm (last visited Oct. 9, 2016). [hereinafter [Year] ODPC Annual Report].

since 2007.[211] In recent years, about half of all those complaints were related to requests by individuals for access to personal data held by a processor.[212] Of 829 complaints resolved in 2014, only 27 resulted in formal decisions by the Commissioner.[213] This very low percentage is typical of recent years.[214]

The annual reports are also full of rather charming case studies involving disputes over data handling that were resolved to the satisfaction of the aggrieved party through some combination of measures such as an apology, the destruction or correction of the person's records, and reform of the offending practice. One illustrative example from 2011, the same year as the ODPC Facebook investigation, concerned a complaint by the user of a gym and swimming pool about the excessive amount of information solicited on a required medical form.[215] The ODPC communicated with the management at the "leisure centre" requesting further information, and then determined that the information collected was "disproportionate" to its purpose, thus violating the Data Protection Act.[216] The facility agreed to make completion of the form optional in the future rather than mandatory, and to destroy existing forms upon request; the complaining party accepted this settlement. The case study concluded: "As a result of this complaint, members of the public may now use the swimming pool at the leisure centre on an anonymous basis and that is as it should be."[217] The 2014 annual report recounted a similar story of a complaint against an apartment broker (called a "letting agency"—the Irish just have better names for things) that collected excessive amounts of data from those merely applying for a rental lease.[218] There again, the agency agreed to change its practices and the case study concluded: "The complainant informed us that she was very satisfied with the outcome of her complaint."[219] These anecdotes add detail to the statistical portrait of an agency primarily concerned with assisting regulated entities in their efforts to comply with the law and helping citizens reach amicable resolutions after violations of their broad data protection rights.

---

211. *See, e.g.*, 2015 ODPC Annual Report, *supra* note 210, at 5 (Commissioner received 932 complaints in 2015, and 960 in 2014); 2013 ODPC Annual Report, *supra* note 210, at 9 (910 complaints in 2013, 1,349 in 2012).

212. *See, e.g.*, 2015 ODPC Annual Report, *supra* note 210, at 5 (60% in 2015); 2013 ODPC Annual Report, *supra* note 210, at 9 (56.8% in 2013). For more on the access right, see *supra* notes 72–75 and accompanying text.

213. *See* 2014 ODPC Annual Report, *supra* note 210, at 6 ("The vast majority of complaints concluded in 2014 were resolved amicably through the efforts of the Office without the need for a formal decision . . . ").

214. *See* 2013 ODPC Annual Report, *supra* note 210, at 10 (29 formal decisions out of 1,290 completed investigations of complaints); 2012 ODPC Annual Report, *supra* note 210, at 9 (36 formal decisions out of 864 completed investigations of complaints); 2011 ODPC Annual Report, *supra* note 210, at 9 (17 formal decisions out of 1,080 completed investigations of complaints).

215. *See* 2011 ODPC Annual Report, *supra* note 210, at 39–40.

216. *Id.*; *see* Irish Data Protection Act, *supra* note 51, § 3 (a).

217. *See* 2011 ODPC Annual Report, *supra* note 210, at 39–40 (Swan Leisure case study).

218. *See* 2014 ODPC Annual Report, *supra* note 210, at 20–21.

219. *Id.*

Finally, in addition to the statistics and case studies from annual reports, statements of ODPC leaders clearly embrace a strategy of responsive regulation. The current Commissioner, Helen Dixon, spent 11 years working in the Irish outposts of U.S. technology companies before becoming a civil servant in various business-related government departments.[220] Since she began the job in late 2014, Dixon has emphasized collaborative techniques as the cornerstone of her approach. In her cover letter in her first ODPC annual report, she expressed her philosophy in terms that sound very much like Ayres and Braithwaite, and thus are worth quoting at length:

> Given the pace and scale of change, I believe it is essential for data-protection authorities to have strong relationships with stakeholders, and regular meaningful dialogue. The engaged approach adopted by my Office means data-protection problems can be detected, and either solved or eliminated, before they affect a greater number of people than would otherwise be the case. . . . Engagement also means that an independent regulator, such as my Office, is better able to guide meaningfully and consistently, over time, the broader development of data protection for the improved benefit of all parties.
>
> Sometimes, of course, effective data-protection regulation is best carried out through the use of our statutory powers. . . . While the explicit use of these tools can be measured, as they are in this report, the implicit threat of their use to ensure compliance is also very useful, though necessarily harder to capture statistically.[221]

In adopting this posture, Dixon is continuing the approach of her predecessor, Hawkes, who served as Commissioner from 2005 to 2014. In his first annual report, he stated:

> Generally, breaches of data protection legislation are unintentional and the majority of data controllers are happy to correct any practices that contravene our legislation.
>
> For the majority of compliant data controllers, my approach is one of helping them to achieve better respect for privacy by offering targeted guidance. For the minority who [wilfully] or carelessly infringe people's privacy rights, my approach is to use the full extent of my powers to achieve quick correction of such behavior.[222]

---

220. *See* Elaine Edwards, *Helen Dixon Appointed as Data Protection Commissioner*, IRISH TIMES (Sept. 10, 2014, 4:43 PM), http://www.irishtimes.com/news/ireland/irish-news/helen-dixon-appointed-as-data-protection-commissioner-1.1924161.

221. 2014 ODPC Annual Report, *supra* note 210, at 2–3.

222. DATA PROT. COMM'R, 2005 ANNUAL REPORT OF THE DATA COMMISSIONER 6, https://www.dataprotection.ie/documents/annualreports/AnnualReport2005-EN.pdf [hereinafter 2005 ODPC Annual Report]. Hawkes has been quoted in other sources discussing similar work. *See* Burrell, *supra* note 2 ("Most of our work is done behind closed doors without publicity but with the outcome being exactly what we want"); Mirani, *supra* note 2 ("Our approach is to talk to companies, explain exactly what we expect of them [and] expect

Statistics, case studies, and policy statements from the regulating authority all demonstrate the pervasive use of responsive privacy regulation by the ODPC. The ODPC found "excessive" data collection by the leisure centre and the letting agency to be unlawful under the Data Protection Act.[223] The same practices by the same types of entities probably would not violate U.S. consumer protection law absent a broken promise, and no other privacy law would be likely to apply. But the fact that the underlying rules are more stringent in Ireland than in the U.S. does not automatically lead to a harsher regulatory response.

What sort of "shotgun behind the door" is available to the ODPC in instances where it must move higher on the regulatory pyramid? Unlike some other E.U. data protection laws, the Irish Data Protection Act does not give the ODPC direct authority to impose financial penalties without judicial participation.[224] This will change under the GDPR, which confers authority on all national data protection regulators to levy very large fines—up to 4% of a company's annual global revenue.[225] That may improve the ODPC's influence over businesses at the top of the responsive regulation pyramid.[226]

Under the Act, the ODPC wields other weapons.[227] Using its investigative powers, the ODPC may inspect the premises and computer systems of data processors at "all reasonable times" and may seize data for investigative purposes.[228] The commissioner also may issue a broad form of subpoena, allowing the ODPC to issue compulsory "information notices" to investigate potential data protection violations.[229] If the ODPC's efforts to reach a reasonable settlement fail, it may issue an "enforcement notice" requiring remedial actions.[230] Typical demands of an enforcement notice might include changes in data practices, staff training, and correction or deletion of the personal data at issue.[231]

---

they will follow that. But if they don't, we have some of the strongest enforcement powers of any European data protection authority.").

223. *See* Irish Data Protection Act 1988, *supra* note 50, § 2(1)(c)(iii); Irish Data Protection Act, *supra* note 51, §3(a).

224. *See* Irish Data Protection Act 1988, *supra* note 50, §31; *see, e.g.*, Lombarte, *supra* note 20, at 124; *Dutch Law Includes General Data Breach Notification Obligation and Larger Fines for Violations of Data Protection Act*, HUNTON & WILLIAMS: PRIVACY & INFO. SECURITY L. BLOG (Jan. 8, 2016), https://www.huntonprivacyblog.com/2016/01/08/dutch-law-includes-general-data-breach-notification-obligation-and-larger-fines-for-violations-of-the-data-protection-act/; Julia Floretti, *German Privacy Regulator Fines Three Firms Over U.S. Data Transfers*, REUTERS (June 6, 2016), http://www.reuters.com/article/us-germany-dataprotection-usa-idUSKCN0YS23H.

225. *See infra* notes 376–78 and accompanying text (explaining new GDPR penalty structure).

226. *See infra* Section V.A.2 (discussing top-of-pyramid penalties in both the United States and Ireland).

227. Hawkes has even called them "some of the strongest enforcement powers of any European data protection authority." Mirani, *supra* note 2.

228. Irish Data Protection Act 1988, *supra* note 50, § 24.

229. *Id*. § 12.

230. *Id*. § 10(2).

231. *See* CAREY, *supra* note 56, at 157.

Failures to cooperate with lawful inspections or to comply with information or enforcement notices are punishable offenses.[232] The ODPC can pursue prosecution of these infractions in court with summary proceedings, which it has done several hundred times over the years.[233] Maximum fines in such cases are limited to either €3,000 or €5,000, depending on the rules violated.[234] An extremely serious case could result in criminal indictment and fines up to €100,000 in ordinary cases and up to €250,000 for violations involving certain electronic privacy rules.[235]

These investigative and enforcement powers are the underpinning of the comprehensive data protection audits the ODPC uses to examine organizations of all sizes.[236] The Facebook investigation discussed in Part IV was such an audit, and the ODPC subsequently conducted a similar audit of LinkedIn.[237] Other audits of companies in recent years have ranged from a trash collection company called Panda Waste to a collection of local credit unions.[238] Government entities, including the national police force and the driver's license bureau, have also been subjected to ODPC audits.[239] In 2014, the ODPC inspected or audited 38 organizations altogether.[240] Overall, the ODPC has relied for leverage on its power to investigate and perhaps ultimately to damage an organization's reputation and goodwill more than on the relatively small and uncommon financial penalties possible under current Irish law.[241]

A final component of responsive regulation is an emphasis on offering education and guidance to help entities bring themselves into compliance with legal requirements.[242] The ODPC devotes considerable resources to these activities. According to the most recent annual report, the ODPC responded to 860 requests for information or assistance with compliance and engaged in 100 more formal consultations with public and private organizations.[243] It publishes multiple guidance documents, including a 16-page booklet entitled *A Guide for Data*

---

232. *See* Irish Data Protection Act 1988, *supra* note 50, §§ 10(9), 12(5), 24(6).

233. *See* CAREY, *supra* note 56, at 156.

234. *Id*. at 161.

235. *Id*.

236. OFFICE DATA PROT. COMM'R, *Guide to Audit Process* 6–7 (Aug. 2014), https://www.dataprotection.ie/docimages/documents/GuidetoAuditProcessAug2014.pdf.

237. *See* Sara Harrington, *Privacy and Data Protection Review of LinkedIn Ireland: Some New Features to Know About*, LINKEDIN: OFFICIAL BLOG (Dec. 18, 2014), https://blog.linkedin.com/2014/12/18/privacy-and-data-protection-review-of-linkedin-ireland-some-new-features-to-know-about.

238. *See* 2014 ODPC Annual Report, *supra* note 210, at 10. (discussing the ODPC's target of local credit unions); 2013 ODPC Annual Report, *supra* note 210, at 25 (noting the ODPC's audit of Panda Waste).

239. *See* 2014 ODPC Annual Report, *supra* note 210, at 10 (discussing the ODPC's audit of An Garda Síochána and the National Driver License Service Center).

240. *Id*. at 5.

241. *See supra* note 233–235.

242. In 1992, Bennett reported that the German data protection regulator "takes pride in the fact that it serves an educative and advisory function." BENNETT, *supra* note 18, at 183.

243. 2015 Annual Report, *supra* note 210, at 12–13.

Controllers, which lays out fundamental principles of data protection law and closes with a checklist for privacy compliance.[244] While the ODPC offers less material than is available on the FTC website, it is clearly a point of emphasis for the ODPC to help regulated parties understand the law, answer their own questions, and improve their compliance voluntarily.

B. The United States: The FTC

As noted before, narrow sectoral statutes in the U.S. give subject-specific regulators the authority to promulgate privacy rules and often create data protection regimes in their areas of expertise. For example, HIPAA authorizes the federal Department of Health and Human Services ("HHS") to regulate data handling by covered healthcare entities, and the Family Educational Rights and Privacy Act ("FERPA") gives the U.S. Department of Education power to regulate student records at public and private educational institutions.[245]

Relying on regulators familiar with the particular concerns of the regulated industry has both advantages and drawbacks. Presumably HHS understands hospitals and the Department of Education understands schools better than an all-purpose DPA, such as the ODPC, understands either. On the other hand, such division can also lead to fragmented power and reinvented wheels. And overlapping authority may cause regulatory competition between agencies, which can have both good and bad effects.[246] The merits of the sectoral approach have been the subject of debate, on which this Article expresses no view. But the differences in national approaches to the issue are consistent with the philosophies discussed in Part I: the E.U. considers data protection a unified area of law protecting a fundamental right, while in the U.S., privacy risk is a characteristic of particular transactions that should be addressed in that context.

For the vast majority of firms that fall outside these more heavily regulated sectors, the U.S. takes a consumer protection approach to privacy, and the preeminent agency enforcing those requirements is the FTC.

Unlike Ireland's Data Protection Act, the structure of the FTC Act does not explicitly instruct the agency to pursue friendly regulatory techniques. If anything, the statute presupposes that the FTC will do most of its work through adversarial enforcement actions. This was especially so after Congress made it prohibitively difficult for the Commission to promulgate regulations interpreting Section 5 in the

---

244. DATA PROT. COMM'R, *Data Protection Acts 1988 and 2003; A Guide for Data Controllers* 3–5, 15, https://www.dataprotection.ie/documents/forms/NewAGuideForDataControllers.pdf.

245. *See* 42 U.S.C. § 1320d-2 (2010) (conferring power to HHS under HIPAA); 20 U.S.C. § 1232(c)(g) (2016) (conferring power to the Department of Education under FERPA).

246. *See generally* REGULATORY COMPETITION AND ECONOMIC INTEGRATION (Daniel C. Esty & Damien Geradin eds., 2001); Francesco Parisi et al., *Two Dimensions of Regulatory Competition*, 26 INTL. REV. L. & ECON. 56 (2004).

ordinary way under the Administrative Procedure Act.[247] That left adjudication as the FTC's primary formal power to police consumer protection violations under Section 5. The FTC nonetheless uses responsive regulation to exercise this authority, both in its approach to enforcement and in its other activities.

The FTC accepts complaints from the public, and may use them to identify enforcement targets or gather evidence.[248] But there is no legal obligation for the FTC to resolve individual complaints; indeed, it warns consumers that it may take no action in response.[249] The FTC can and does commence investigations on its own initiative, or at the suggestion of the target company's competitors.[250] Like the ODPC, the FTC has a range of information-gathering techniques at its disposal, including voluntary requests (backed, of course, by the implied threat of punitive action and the desire of the target company to engender goodwill) and various forms of compulsory process.[251]

Enforcement actions concerning privacy and security routinely result in negotiated agreements with the targeted company.[252] In recent years, just three companies have chosen to dispute the FTC's privacy or security claims before a judge (either in an administrative process or in district court)[253]—out of some 170 such complaints.[254] All the others accepted consent decrees creating binding legal obligations, which generally include ongoing FTC review of the company's compliance. The FTC's formal procedures for the formation and content of consent orders are rather skeletal.[255] In practice, the informal negotiations center on remedial actions. The FTC has developed stock language for the remedies commonly included in consent decrees, particularly for a company's adoption of a 20-year "privacy compliance program" that incorporates dedicated management of privacy

---

247. *See* HOOFNAGLE, *supra* note 15, at 101–02. The FTC can write regulations in the traditional manner when using its authority under other statutes, such as COPPA. *See generally* 16 C.F.R. pt. 312 (2015).

248. *See Submit a Consumer Complaint to the FTC*, FED. TRADE COMMISSION, https://www.ftc.gov/faq/consumer-protection/submit-consumer-complaint-ftc (last visited Nov. 11, 2016).

249. *Id*.

250. *See* HOOFNAGLE, *supra* note 15, at 103.

251. *See id*. at 105–09.

252. *See id*. at 111; Solove & Hartzog, *supra* note 15, at 606, 610.

253. Two of the cases ended in rulings by federal appeals courts upholding the FTC's power over privacy and security. *See* FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 257 (3d Cir. 2015) (rejecting a challenge to FTC authority over data security under Section 5); FTC v. Accusearch, Inc., 570 F.3d 1187, 1194 (10th Cir. 2009) (holding that the FTC may enforce Section 5 against unfair trade practices whether or not those practices also violate other provisions of law). The third case went through the administrative process within the FTC. *In re* LabMD, Inc., No. 9357, 2016 WL 4128215, at *32 (F.T.C. July 28, 2016) (overturning an administrative law judge who had ruled that the FTC failed to prove an unfair trade practice arising from inadequate data security and imposing a remedial order). An appeal of the third case is now pending in the Eleventh Circuit.

254. Solove & Hartzog, supra note 15, at 610.

255. *See* 16 C.F.R. §§2.31–2.34 (requiring an agreement to cease and desist and stating that the FTC may establish compliance procedures).

compliance, development of policies, periodic outside audits, and access for the FTC to inspect continued adherence to the program.[256]

These FTC techniques adhere closely to Ayres and Braithwaite's pyramid model for responsive regulation. The regulatory agency acts under the starting assumption that the regulated party intends to do its best to comply with the law. Initial contacts are often voluntary and oriented toward remediation. The resolution for a first offense is worked out privately between FTC staff and the target of the investigation; the complaint and the consent decree typically are unveiled simultaneously, and although the public may comment on the proposed remedy, in practice this is just a formality before the ratification of the agreed settlement.[257]

Once a company is under a consent decree—and remember, 20-year durations are common—the FTC gains greater leverage, moving that company, which has failed once, higher up the pyramid. The ongoing internal compliance program and outside audits, along with the FTC's power to inspect them, combine to put the company on a sort of probation. Crucially, although the FTC cannot impose fines for violations of Section 5, once a company is under a consent decree, subsequent violations of the consent decree carry potentially significant fines: $16,000 per individual violation, which might be multiplied by thousands or even millions of users, and levied on a daily basis for continuing violations.[258]

Google learned about graduated penalties in the responsive regulation pyramid the hard way. In October 2011, just before the Facebook settlement discussed in Part IV, Google accepted a consent decree concerning privacy violations in the rollout of Google Buzz, one of its several failed attempts to develop a social networking platform.[259] That order rather broadly required that Google not "misrepresent in any manner, expressly or by implication . . . the extent to which respondent maintains and protects the privacy and confidentiality of any covered information . . . ."[260] Ten months later, the FTC reached a new settlement with Google, this time for falsely stating that it respected a default setting in the Safari browser that blocked certain third-party cookies.[261] The complaint in the second action did not base liability on a violation of Section 5, although certainly a deceptive practices claim might have been brought in the circumstances. Rather, the FTC accused Google of violating the previous consent order.[262] Because this second infraction was now subject to a fine, Google was forced to pay a civil monetary

256. *See, e.g.*, *In re* Snapchat, No. C-4501, 2014 WL 7495798, at *7–11 (F.T.C. Dec. 23, 2014) (consent order); *In re* Facebook, No. C-4365, 2012 WL 3518628, at *79–83 (F.T.C. Aug. 10, 2012) (consent order) [hereinafter FTC Facebook Order], *In re* Google, 152 F.T.C. 435 (2011), 2011 WL 11798458, at *9–12 (consent order).

257. *See* HOOFNAGLE, *supra* note 15, at 111 ("The FTC politely acknowledges public comment, but such comment almost never alters the settlement agreement.").

258. *See* 16 C.F.R. § 1.98(c); HOOFNAGLE, *supra* note 15, at 115.

259. In re *Google*, 2011 WL 11798458, at *1–5.

260. *Id*. at *5.

261. United States v. Google, No CV12-04177SI, 2012 WL 5833994, at *1 (N.D. Cal. Nov. 16, 2012).

262. Compl. Civil Remedies at ¶¶ 51, 54, 57, United States v. Google, 2012 WL 5833994 (2012) (No. CV12-04177SI), 2012 WL 3234957.

penalty of $22.5 million as part of the settlement.[263] The chair of the FTC sounded the theme of graduated penalties in a statement about the second enforcement action:

> The record setting penalty in this matter sends a clear message to all companies under an FTC privacy order. No matter how big or small, all companies must abide by FTC orders against them and keep their privacy promises to consumers, or they will end up paying many times what it would have cost to comply in the first place.[264]

While more study would be necessary to test this theory, it is quite plausible that the lack of a monetary penalty in the first enforcement action *encourages* settlement. A company facing the prospect of a significant fine might logically expend legal fees to fight the FTC.[265] Instead, the cost of any such dispute naturally exceeds the zero direct penalty that the company would be charged. There are other incentives, of course.[266] A company reduces uncertainty by settling, and even gains some influence over its future obligations through the negotiations over terms. Furthermore, by biting the bullet and settling, a company can reduce the public relations damage caused by public airing of government accusations of poor data-handling practices, enduring just one bad story in the press instead of a protracted dispute. Finally, because consent decrees invariably allow the company not to admit fault, they can reduce both reputational harm and the risk of subsequent legal liability.

Whatever the incentives to settle, once a company has done so, it finds itself higher on the regulatory pyramid—subject to greater oversight, more specific obligations, and more significant financial penalties for future privacy failures. The FTC has methodically reached consent decrees with many digital technology firms, including not only Facebook and Google, but also Microsoft, Twitter, Snapchat, and Oracle, to name a few.[267] By accumulating consent decrees, the FTC has entrenched its role as a regulatory auditor, which encourages companies, in turn, to develop internal compliance mechanisms.[268]

Over time, the violations alleged in FTC complaints and the conditions established in consent decrees offer other regulated companies a picture of the Commission's expectations concerning privacy and security.[269] Steven Hetcher explained the early FTC embrace of online privacy policies as a form of norm

---

263. *Google*, 2012 WL 5833994, at *2.

264. Press Release, FTC, Google Will Pay $22.5 Million to Settle FTC Charges it Misrepresented Privacy Assurances to Users of Apple's Safari Internet Browser (Aug. 9, 2012), https://www.ftc.gov/news-events/press-releases/2012/08/google-will-pay-225-million-settle-ftc-charges-it-misrepresented (quoting FTC Chair Jon Leibowitz).

265. *See* Solove & Hartzog, *supra* note 15, at 611–12 (noting this possibility).

266. *See* HOOFNAGLE, *supra* note 15, at 111 (considering reasons for companies to settle with the FTC).

267. *See Cases and Proceedings: Advanced Search*, FED. TRADE COMMISSION https://www.ftc.gov/enforcement/cases-proceedings/advanced-search (input name of company in Search box) (last visited Oct. 10, 2016).

268. *See* Cohen, *supra* note 15, at 27.

269. *See* Solove & Hartzog, *supra* note 15, at 607–08 (arguing that this system resembles common law).

entrepreneurship that simultaneously defined privacy responsibilities for companies and expanded the FTC's power.[270] These consent decrees work in just the same way by establishing new expectations for privacy, for both the specific target companies and others,[271] and solidifying the FTC's enforcement authority over them. New consent decrees are major events within the emerging specialized privacy compliance bar in the U.S., whose members assiduously analyze them. This role for settlements helps to address any concerns that individualized resolutions under responsive regulation might not establish clear and universally applicable legal standards.[272]

Regulatory resources are always constrained, of course. Like all enforcement agencies, the FTC must prioritize its cases, and an examination of its chosen targets demonstrates some discernible and predictable patterns. The Commission tends to go after larger companies (whose shortcomings affect the most consumers), the most egregious offenses (which may be especially likely to cause harm, and where enforcement action would be especially important to proscribe as a warning to other firms), and infractions involving children's privacy (where there is also heightened harm, as well as clearer political consensus, and additional FTC powers under COPPA). In other words, FTC enforcement targets the big guys, the bad guys, and those who harm kids.[273] The need to prioritize enforcement is part of all regulatory approaches, not just the responsive ones, but it means that complaints and consent decrees can only do part of the FTC's job in policing privacy.

Consistent with the responsive regulation model, the FTC also issues a significant quantity of guidance materials to help businesses understand their legal responsibilities for privacy and security. For example, while the FTC was investigating Facebook (and Google), it was completing a final version of a sweeping report concerning privacy recommendations for companies. To create this report, the FTC began with a series of roundtables in 2009 and 2010, leading to a proposed staff report published for comment at the end of 2010.[274] The final report was issued in March 2012, months after the Facebook settlement.[275] While it offered

---

270. *See* Hetcher, *supra* note 18, at 2062.

271. *See* Solove & Hartzog, *supra* note 15, at 619–25 (arguing that this system resembles common law).

272. *See supra* note 174 and accompanying text.

273. *See* MCGEVERAN, *supra* note 23, at 225. Cases involving a combination of these factors are even more attractive to the FTC. The complaint against Snapchat involved all three: an estimated 100 million users, including a large percentage of minors, who were assured repeatedly that the recipients of pictures sent through the app could not retain them despite multiple widely known methods to do just that. *See* Compl., *In re* Snapchat, (F.T.C. Dec. 23, 2014) (No. C-4501) 2014 WL 7495798, at *7–11, https://www.ftc.gov/system/files/documents/cases/141231snapchatcmpt.pdf.

274. *See FTC Privacy Report*, FED. TRADE COMMISSION, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/ftc-privacy-report (last visited Oct. 10, 2016).

275. Press Release, FTC, FTC Issues Final Commission Report on Protecting Consumer Privacy (March 26, 2012), https://www.ftc.gov/news-events/press-releases/2012/03/ftc-issues-final-commission-report-protecting-consumer-privacy; *see* FTC, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR

a broad set of standards rather than detailed regulations, the 2012 FTC Report emphasized the importance of developing new products, services, and features with consideration of privacy from the earliest stages (so-called "privacy by design"[276]), meaningful choice for consumers, and transparency and consistency about privacy practices.[277] The report emphasized industry "best practices" rather than formal legal compliance measures, maintained flexibility in the face of changing technology, and drew insights from engagement with stakeholders to develop legal expectations collaboratively.[278]

The 2012 FTC Report was a particularly ambitious effort to provide guidance for businesses and their lawyers, but certainly not the only one. The FTC website houses a "Business Center" with a separate page offering advice for companies about privacy and security issues, ranging from two-minute videos and short documents highlighting key issues, to a blog, to summaries of recent cases that emphasize the takeaway points for other companies so they can avoid committing the same violations.[279] Two comprehensive but user-friendly guides for businesses summarize best practices for data privacy and data security.[280] The FTC has also convened over 35 topical workshops about privacy issues in the last 20 years and issued dozens of reports.[281] Recent workshops and reports tended to focus on emerging topics such as cross-device tracking[282] or so-called "Big Data" analysis[283] of personal information.

In summary, despite an authorizing statute that envisions primarily adversarial enforcement actions, the FTC has embraced responsive regulation of privacy at U.S.-based companies. It has thus emerged as the preeminent privacy

---

BUSINESSES AND POLICYMAKERS (March 2012), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf [hereinafter 2012 FTC Report].

276. *See generally* Ira Rubinstein, *Regulating Privacy by Design*, 26 BERKELEY TECH. L.J. 1409 (2012).

277. 2012 FTC Report, *supra* note 275, at 23–71.

278. *Id*. at 16; *see* Thaw, *supra* note 15, at 336–42 (evaluating consultative elements of FTC data security enforcement).

279. The business-oriented materials span multiple interlinked pages, but for a good starting point see *Privacy and Security*, FED. TRADE COMMISSION, https://www.ftc.gov/tips-advice/business-center/privacy-and-security (last visited Oct. 10, 2016).

280. *See Protecting Personal Information: A Guide for Business*, FED. TRADE COMMISSION (Nov. 2011), https://www.ftc.gov/sites/all/libraries/infosecurity/; FTC, START WITH SECURITY; A GUIDE FOR BUSINESS (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

281. *See* FTC, PRIVACY & DATA SECURITY UPDATE: 2015 at 13–14, https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2015/privacy_and_security_data_update_2015-web_0.pdf.

282. *See, e.g*., *Cross-Device Tracking*, FED. TRADE COMMISSION (Nov. 16, 2015), https://www.ftc.gov/news-events/events-calendar/2015/11/cross-device-tracking.

283. *See, e.g.*, Press Release, FTC, FTC Report Provides Recommendations to Business on Growing Use of Big Data (Jan. 6. 2016), https://www.ftc.gov/news-events/press-releases/2016/01/ftc-report-provides-recommendations-business-growing-use-big-data.

regulator in the United States, even though it did so using consumer protection powers that have no particular focus on the handling of personal data.

IV. FACEBOOK: FRIENDING THE REGULATORS

In 2011, regulators in both the United States and Ireland conducted wide-ranging enforcement actions related to Facebook's information-handling practices. The FTC reached a settlement with Facebook and then simultaneously announced to the public its complaint and a consent decree with a 20-year duration.[284] Meanwhile, the ODPC completed an audit of Facebook-Ireland, and released its comprehensive results, documenting a series of required improvements in Facebook's practices and deadlines for their implementation.[285] These two regulatory interventions, conducted simultaneously and completed within weeks of one another, make a good comparative case study. They demonstrate the twin theses of this Article: that a responsive regulation approach blurs the distinctions between otherwise divergent substantive privacy law, and that it can be an effective method to improve data practices.

Around the world, the law has struggled to deal with social media, particularly Facebook. Anupam Chander has shown that Facebook's breathtaking global scale and nearly unique degree of interactivity often prompt people to use the language of nationhood to describe it, and to ask: "Who rules Facebookistan?"[286] The answer is complex, both because the platform governs itself to a great degree through the design of its interface and its terms of use,[287] and because the relevant jurisdictional rules can be extremely complex.[288] Chander chronicles a number of attempts by legal systems in various nations to assert their authority over Facebookistan, including not only the United States and Ireland, but also Germany, France, Canada, China, Syria, Tunisia, and Egypt.[289] A comprehensive investigation of privacy on Facebook by the Canadian Privacy Commissioner, completed in 2009, presaged the findings of the FTC and ODPC in many respects.[290] More recently,

---

284. *See* Compl., *In re* Facebook, (2012) (No. C-4365), 2012 WL 3518628, https://www.ftc.gov/sites/default/files/documents/cases/2011/11/111129facebookcmpt.pdf [hereinafter FTC Facebook Complaint]; FTC Facebook Order, *supra* note 256. The agreement was announced on Nov. 29, 2011. Press Release, FTC, Facebook Settles FTC Charges That It Deceived Consumers by Failing to Keep Privacy Promises (Nov. 29, 2011), https://www.ftc.gov/news-events/press-releases/2011/11/facebook-settles-ftc-charges-it-deceived-consumers-failing-keep.

285. ODPC Facebook Audit, *supra* note 196, at 3–20.

286. ANUPAM CHANDER, THE ELECTRONIC SILK ROAD 113–14 (2013).

287. *See generally* LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE (1999); Joel R. Reidenberg, *Lex Informatica*: *The Formulation of Information Policy Rules Through Technology*, 76 TEX. L. REV. 553 (1997).

288. *See* KUNER, *supra* note 22, at 109–35.

289. CHANDER, *supra* note 286, at 120–31.

290. *See generally* ELIZABETH DENHAM, ASSISTANT PRIVACY COMM'R OF CAN., REPORT OF FINDINGS INTO THE COMPLAINT FILED BY THE CANADIAN INTERNET POLICY AND PUBLIC INTEREST CLINIC (CIPPIC) AGAINST FACEBOOK INC. UNDER THE PERSONAL INFORMATION PROTECTION AND ELECTRONIC DOCUMENTS ACT (July 16, 2009), https://www.priv.gc.ca/cf-dc/2009/2009_008_0716_e.asp.

Facebook prevailed in an appeals court in its challenge against an enforcement action by Belgium's data protection regulator.[291] Given Facebook's vast scale, many nations will attempt to influence its operations by asserting legal claims against it. Responsive regulatory techniques offer a desirable method for doing so.

Facebook has always faced criticism and legal challenges over its information-handling practices, even before it grew into "Facebookistan." That was already evident in the company's infancy, when it was still available almost exclusively to high school and college students, as explained by *Time Magazine* in 2006:

> On Tuesday morning the popular social networking site unrolled a new feature dubbed the "News Feed" that allows users to track their friends' Facebook movements by the minute. For many of Facebook's 8 million-plus student users, it was too much. Within 24 hours, hundreds of thousands of students nationwide organized themselves to protest the new feature. Ironically, they're using Facebook to do it.[292]

Ten years later, of course, Facebook has quite a few more than eight million users around the world, of all ages.[293] News Feed, the continuous stream of items posted by friends (and other sources chosen by the user), replaced an interface that required a user to visit each friend's profile page individually to see the latest updates. It has since become a defining feature of the interface that helped fuel the social network's growth, now so central that it is difficult to imagine Facebook functioning without it.[294]

---

291. *See* Stephanie Bodoni & Aoife White, *Facebook Wins Belgian Court Case Over Storing Non-User Data*, BLOOMBERG TECH. (June 29, 2016), http://www.bloomberg.com/news/articles/2016-06-29/facebook-wins-belgian-court-appeal-over-storing-non-user-data. The Belgian case involved the collection of aggregate data about the activities of nonusers through Facebook's "Like" buttons on other websites, see *id*., which was also considered in the ODPC Facebook Audit, see *supra* note 196, at 81–83, and previously had been the subject of enforcement actions by German state regulators, see CHANDER, *supra* note 286, at 122–24.

292. Tracy Samantha Schmidt, *Inside the Backlash Against Facebook*, TIME (Sept. 6, 2006), http://content.time.com/time/nation/article/0,8599,1532225,00.html (describing the formation of Facebook user groups to protest the News Feed and criticism in college newspapers).

293. Facebook claims to have "1.71 billion monthly active users as of June 30, 2016" and estimates that "84.5% of [its] daily active users are outside the US and Canada." *See Newsroom: Stats*, FACEBOOK, http://newsroom.fb.com/company-info/ (last visited Oct. 21, 2016).

294. *See* Caitlin Dewey, *After Eight Years With Facebook's News Feed, There's No Such Thing As 'TMI,'* WASH. POST (Sept. 23, 2014), https://www.washingtonpost.com/news/the-intersect/wp/2014/09/23/after-eight-years-with-facebooks-news-feed-theres-no-such-thing-as-tmi/; Farhad Manjoo, *Facebook News Feed Changed Everything*, SLATE (Sept. 12, 2013), http://www.slate.com/articles/technology/technology/2013/09/facebook_news_feed_turns_7_why_it_s_the_most_influential_feature_on_the.html.

This early controversy over the News Feed exemplifies the broader problem technology presents for privacy regulators: it is a fast-moving target. The designers of every platform continually experiment with the organization and distribution of personal information—including not only Facebook's 2006 changes, but such recent examples as LinkedIn sending emails to people in new members' contact lists inviting them to join the service or Twitter's experimentation with new algorithmic sorting in users' feeds.[295]

"Privacy lurches" can disorient users and depart from their expectations.[296] If new policies contradict previous commitments about privacy, the changes may well be illegal under a consumer protection model. If they move beyond legitimizing conditions, they might violate data protection law. These sorts of changes increase the risks of accidental disclosures to unintended audiences—what human-computer interaction scholar Kelly Caine calls "misclosures"[297]—that are already common when using highly networked platforms with complicated interfaces, such as Facebook.

Yet heavy-handed legal intervention against the shift to the News Feed would have thwarted an innovation that has proven itself valuable to both the company and its customers. The change was controversial at the time because, even though personal information posted on a profile was still visible to exactly the same audience of approved friends, making it much more readily accessible reduced users' "privacy by obscurity."[298] The company exacerbated the problem by failing to recognize these privacy implications and rolling out the new feature too quickly, with too little warning, and with an attitude that suggested its users' reservations were foolish.[299] Over time, however, users have adjusted to the shift in information flows and learned how to protect their privacy. They certainly did not, as some observers predicted at the time, leave the service in droves.[300] Regulators must leave

---

295. Perkins v. Linkedin Corp., 53 F. Supp. 3d 1222, 1255 (N.D. Cal. 2014) (rejecting motion to dismiss class action lawsuit concerning LinkedIn's practices in sending reminder emails); Doug Bolton, *Twitter is Experimenting with Putting Tweets Out of Order in Users' Timelines*, INDEPENDENT (Dec. 8, 2015), http://www.independent.co.uk/life-style/gadgets-and-tech/news/twitter-timeline-out-of-order-test-experiment-a6765371.html.

296. *See* Paul Ohm, *Branding Privacy*, 97 MINN. L. REV. 907, 915–16 (2013).

297. Kelly E. Caine, *Supporting Privacy by Preventing Misclosure*, CHI '09 EXTENDED ABSTRACTS HUM. FACTORS COMPUTING SYS. 3145, *3147 (2009).

298. *See generally* Woodrow Hartzog & Fred Stutzman, *The Case for Online Obscurity*, 101 CAL. L. REV. 1 (2013).

299. Facebook founder Mark Zuckerburg infamously responded to the uproar with a somewhat snarky blog post defending the changes, entitled "Calm down. Breathe. We Hear You." Mark Zuckerburg, *Calm Down. Breathe. We Hear You*., FACEBOOK (Sept. 5, 2006), https://www.facebook.com/notes/facebook/calm-down-breathe-we-hear-you/2208197130/ ("[W]e agree, stalking isn't cool; but being able to know what's going on in your friends' lives is. . . . Nothing you do is being broadcast; rather, it is being shared with people who care about what you do—your friends.").

300. *See* Claudine Beaumont, *'Quit Facebook' Protest Day Flops*, TELEGRAPH (June 1, 2010, 11:20 AM), http://www.telegraph.co.uk/technology/facebook/7792970/Quit-Facebook-protest-day-flops.html. Clearly, the staggering growth of the platform belies any notion that privacy objections are driving away consumers in large numbers. For those who

companies enough room to experiment, and users enough time to adjust, or risk thwarting desirable improvements.

Facebook made another lurching change the next year that probably did merit legal intervention. An initiative called Facebook Beacon allowed the social network's advertising partners to disclose information about a person's online activities outside of Facebook on the News Feeds of that person's friends inside of Facebook.[301] This type of "frictionless sharing," which transmits automated messages into Facebook by default rather than by a conscious user action, raises many serious problems, including the risk of misclosures, the commercialization of individual identity, and the "spammification" of user recommendations that undermines their usefulness.[302] The backlash against Beacon was intense and Facebook quickly reversed course.[303] Founder Mark Zuckerburg later admitted the entire effort was a mistake.[304] Class action lawsuits, based in large part on state consumer protection law, soon followed; the company settled them promptly for $9.5 million.[305] U.S. regulators like the FTC took no public action as this dispute unfolded, despite the clear privacy problems caused by Beacon.

The News Feed and Beacon controversies were the prologues to the investigations by the ODPC and FTC, which generally focused on activities between 2009 and 2011. As illustrated by the two examples just discussed, Facebook had exhibited a somewhat cavalier attitude about user data and a tendency toward privacy lurches. It was also clear, however, that the social network was an evolving concept and that a heavy-handed regulatory approach could forestall innovation and create other problems. The two countries' regulators acted against that backdrop.

---

do leave, there is conflicting empirical research about the significance of privacy among their motivations. *Compare* Lee Rainie et al., PEW INTERNET & AM. LIFE PROJECT, COMING AND GOING ON FACEBOOK 2 (Feb. 5, 2013), http://www.pewinternet.org/files/old-media//Files/Reports/2013/PIP_Coming_and_going_on_facebook.pdf (finding that 61% of Facebook users took a break from using the service, but that only 4% of that group cited concerns related to privacy, security, advertising, or spam as the reason), *with* Stefan Stieger et al., *Who Commits Virtual Identity Suicide? Differences in Privacy Concerns, Internet Addiction, and Personality Between Facebook Users and Quitters*, 16 CYBERPSYCHOLOGY, BEHAV. & SOC. NETWORKING 629, 629 (2013) (finding in study of people who had stopped using Facebook that nearly half identified privacy concerns as a reason, by far the most frequently offered explanation).

301. *See* Louise Story & Brad Stone, *Facebook Retreats on Online Tracking*, N.Y. TIMES, Nov. 30, 2007, at C1.

302. *See* William McGeveran, *The Law of Friction*, 2013 U. CHI. LEGAL F. 15, 39–49.

303. *See* Bobbie Johnson, *Facebook Backs Down Over Controversial Advertising System*, GUARDIAN (Nov. 30, 2007), http://www.theguardian.com/technology/2007/nov/30/facebook.beacon; Story & Stone, *supra* note 301.

304. *See* Peter Kafka, *Facebook CEO Mark Zuckerberg: Yep, Beacon Was a Mistake*, BUS. INSIDER (May 28, 2008), http://www.businessinsider.com/2008/5/live-facebook-ceo-mark-zuckerberg-at-d.

305. *See, e.g.*, Lane v. Facebook, Inc., 696 F.3d 811, 816–17 (9th Cir. 2012).

In December 2009, Facebook changed its architecture again and adjusted its privacy policies accordingly.[306] As summarized later in the FTC's complaint, several of these changes altered the categories of personal information over which users could restrict access, converting some to "publicly available" when users previously could set those same categories as "visible" only to their friends or to "friends of friends."[307] Meanwhile, some types of information became more readily accessible to the makers of applications that run within Facebook, and the unique Facebook ID was available to some advertisers—all allegedly with inadequate disclosures of these facts by Facebook.[308] Moreover, some of these changes automatically superseded previous user privacy settings that were stricter.[309] Facebook implemented the modifications by requiring every user to click through a "Privacy Wizard" interface confirming privacy settings, but the FTC objected that the Wizard presented the new policies in a misleading way.[310] Some of these policy revisions were controversial immediately; privacy advocacy groups such as the Electronic Privacy Information Center called on the FTC to investigate.[311]

As noted earlier, FTC privacy cases almost always settle, resulting in no fine for a first infraction but requiring improvements in data-handling practices and long-term FTC monitoring and internal compliance programs.[312] That is exactly what happened after the FTC presented its complaint to Facebook. Like many other privacy consent decrees entered by the FTC, Facebook's also had a 20-year term, and it obliged Facebook to establish a "comprehensive privacy program," to conduct biennial audits of its privacy performance, and to make certain records available to the FTC on request.[313] In another resemblance to typical FTC consent decrees, Facebook did not admit wrongdoing.

What sets the Facebook Order apart from most other consent decrees is a set of conditions that the company "clearly and prominently" announce changes to the mechanisms for disclosing users' personal information.[314] The consent decree includes detailed requirements for these announcements, drawn from the FTC's consumer-protection expertise.[315] Facebook would not be subject to similar

---

306. *See* Bobbie Johnson, *Facebook Privacy Change Angers Campaigners*, GUARDIAN (Dec. 10, 2009), https://www.theguardian.com/technology/2009/dec/10/facebook-privacy.

307. *See* FTC Facebook Complaint, *supra* note 284, at ¶¶ 19–22.

308. *Id*. at ¶¶ 30–40.

309. *Id*. at ¶ 21.

310. *Id*. at ¶¶ 23–24.

311. *See* Johnson, *supra* note 306; Brad Stone, *Privacy Group Files Complaint on Facebook Changes*, N.Y. TIMES: BITS BLOG (Dec. 17, 2009), http://bits.blogs.nytimes.com/2009/12/17/privacy-group-files-complaint-on-facebook-privacy-changes.

312. *See supra* notes 252–56 and accompanying text.

313. *See* FTC Facebook Order, *supra* note 256, at *79–83.

314. *Id*. at *79.

315. *Id*. at *78. For example, the consent decree specifies that disclosures "in textual communications (e.g., printed publications or words displayed on the screen of a computer or mobile device)" must be "of a type, size, and location sufficiently noticeable for

restrictions under the FTC's normal jurisdiction, so in effect, the Commission used the settlement as leverage to increase Facebook's substantive privacy responsibilities for the following two decades. And, as usual, failure to meet these heightened duties can now trigger a potentially significant fine.[316]

Meanwhile, Facebook's practices during the post-Beacon period were of particular interest to the ODPC, because the company opened its European headquarters in Dublin in 2008. After opening this subsidiary in Ireland, Facebook altered its terms of service so that its contractual relationship with all users outside the United States and Canada connected them to the Facebook-Ireland subsidiary, rather than to the main U.S.-based company.[317] There are now over 1,000 employees in Facebook's Dublin office, the biggest concentration outside its global headquarters in Silicon Valley.[318] Under the current Data Protection Directive, the presence of this rest-of-world headquarters gives Ireland primary jurisdiction over the company's data-handling practices.[319]

According to the ODPC, it unilaterally selected Facebook for a comprehensive data protection audit at the beginning of 2011.[320] In August and September of that year, a privacy advocacy group called Europe Versus Facebook filed a series of 22 specific complaints about Facebook with the Commissioner.[321] Europe Versus Facebook was created by Maximilian Schrems, the Austrian privacy

---

an ordinary consumer to read and comprehend them, in print that contrasts highly with the background on which they appear." *Id*.

316. *See supra* note 258 and accompanying text.

317. *See* ODPC Facebook Audit, *supra* note 196, at 21.

318. *See* Linsey Barber, *In Pictures: Inside Facebook's New Dublin Office and European HQ*, CITY A.M. (June 17, 2014, 2:56 PM), http://www.cityam.com/blog/1403013362/inside-facebooks-new-european-hq-pictures (nothing the Dublin office is the largest Facebook office outside the Silicon Valley); Pamela Newenham, *Facebook's Irish Boss Accentuates the Positive*, IRISH TIMES (Oct. 9, 2015), http://www.irishtimes.com/business/technology/facebook-s-irish-boss-accentuates-the-positive-1.2383770.

319. *See* KUNER, *supra* note 22, at 117–18. The default rule under the Directive uses the location of the establishment of a data controller as the primary jurisdiction. *See* E.U. Data Protection Directive, *supra* note 44, art. 4, §1(a). The GDPR will continue that general default rule, subject to some new oversight mechanisms. *See* GDPR, *supra* note 13, arts. 4, §16(b), 56, §1; *see also infra* notes 379–85 and accompanying text (discussing national regulators' role under the GDPR).

320. *See* ODPC Facebook Audit, *supra* note196, at 22.

321. The Europe Versus Facebook webpage includes links to all 22 complaints along with other documents related to its campaign against Facebook within the ODPC. *Legal Procedure Against Facebook Ireland Limited*, EUROPE VERSUS FACEBOOK, http://www.europe-v-facebook.org/EN/Complaints/complaints.html (last visited Oct. 22, 2016).

activist who colorfully criticized Ireland as the Cayman Islands of the data barons.[322] These complaints were absorbed into the audit as well.[323]

The ODPC Facebook Audit laid out a detailed set of changes and improvements in Facebook's data practices. The regulator and the company negotiated over the list, and in the end, Facebook accepted the recommended improvements.[324] One of the major areas concerned the clarity of disclosures made to users, especially in light of the complexity of Facebook's privacy settings and retroactive changes in them—precisely the issues central to the FTC inquiry. In response, Facebook agreed to increase its transparency to users, with continued follow-up from the ODPC to ensure that the improvements are sufficient.[325] In some instances, such changes were spelled out in great detail: for the then-novel feature of suggested photo tags based on facial recognition, for example, Facebook was required to provide additional notice to users under the following guidelines:

> [The notice] will appear at the top of the page when a user logs in. If the user interacts with it by selecting either option presented then it will disappear for the user. If the user does not interact with it then it will appear twice more for a total of 3 displays on the next successive log-ins.[326]

Finally, like the FTC, the ODPC established an ongoing process for monitoring compliance. As a start, the regulator conducted a follow-up audit the next year to assess Facebook's progress toward promised improvements.[327] It found that "most of the recommendations have been implemented to [the ODPC's] satisfaction" and for the remainder it provided detailed work plans for Facebook to cooperate with the ODPC in meeting those goals by specified deadlines.[328]

Overall, the ODPC was sufficiently satisfied with the results of its interactions with Facebook to use the same model again in 2014, when it completed a similar audit of the Irish headquarters of another social networking platform, LinkedIn.[329] Dixon has indicated her intention for the ODPC to conduct similar audits of Apple, Adobe, and Yahoo! in the near future.[330]

---

322. *See supr*a note 3 and accompanying text. For more about Schrems, see Kashmir Hill, *Max Schrems: The Austrian Thorn in Facebook's Side*, FORBES (Feb. 7, 2012), http://www.forbes.com/sites/kashmirhill/2012/02/07/the-austrian-thorn-in-facebooks-side/.

323. *See* ODPC Facebook Audit, *supra* note 196, at 22.

324. *See id*. at 5–20.

325. *Id*.

326. *Id*. at 105.

327. See DATA PROT. COMM'R, FACEBOOK IRELAND LTD.: REPORT OF RE-AUDIT (Sept. 21, 2012), https://dataprotection.ie/documents/press/facebook_ireland_audit_review_report_21_sept_2012.pdf [hereinafter ODPC Facebook Re-Audit].

328. *Id*. at 3–4.

329. *See* 2014 ODPC Annual Report, *supra* note 210, at 10.

330. *See* Conor Humphries, *Irish Regulator of Apple, Facebook Eyes Power To Levy Huge Fines*, REUTERS (Feb. 19, 2015), http://www.reuters.com/article/us-eu-dataprotection-ireland-interview-idUSKBN0LL1PF20150219. The ODPC conducted 51

Understandably, Facebook presented the results of the two investigations in the best possible light. It is intriguing how closely the company's statements adhere to the responsive regulation playbook. In a long blog post the day the FTC settlement was announced, Zuckerberg cast it in terms of dialogue and improvement and pointedly placed Facebook alongside other large digital technology companies:

> As we have grown, we have tried our best to listen closely to the people who use Facebook. We also work with regulators, advocates and experts to inform our privacy practices and policies. Recently, the [FTC] established agreements with Google and Twitter that are helping to shape new privacy standards for our industry. Today, the FTC announced a similar agreement with Facebook. These agreements create a framework for how companies should approach privacy in the United States and around the world.
>
> For Facebook, this means we're making a clear and formal long-term commitment to do the things we've always tried to do and planned to keep doing—giving you tools to control who can see your information and then making sure only those people you intend can see it.[331]

Notice in particular how this statement envisions a cooperative effort between the regulator and companies to "shape new privacy standards for our industry."[332] Facebook, by friending the FTC, is pulling it closer. In return, however, the FTC gets powerful influence over the design of privacy rules throughout the industry. When discussing the Irish audit, a senior official at Facebook-Ireland similarly emphasized areas where the ODPC found its practices laudable:

> Of course, Facebook is always looking to improve our privacy policies and practices, and the [ODPC's] review of our existing operations highlighted several opportunities to strengthen our existing practices. Facebook has committed to either implement, or to consider, other "best practice" improvements recommended by the [ODPC], even in situations where our practices already comply with legal requirements.[333]

Again, the ethos of responsive regulation permeates this statement. Rather than focusing on the specific details of rules, Facebook highlights advice from and communication with the ODPC and describes improvements as steps toward best

---

audits and inspections in 2015. *See* 2015 ODPC Annual Report, *supra* note 210, at 10. It reportedly began an audit of Adobe in 2016. *See* Adrian Weckler, *Facebook Forced to Introduce New Privacy Settings by Irish Authorities*, INDEPENDENT.IE (June 21, 2016), http://www.independent.ie/business/technology/facebook-forced-to-introduce-new-privacy-settings-by-irish-authorities-34819193.html.

331. Mark Zuckerburg, *Our Commitment to the Facebook Community*, FACEBOOK (Nov. 29, 2011), https://newsroom.fb.com/news/2011/11/our-commitment-to-the-facebook-community/.

332. *Id*.

333. Richard Allan, *Facebook and the Irish Data Protection Commission*, FACEBOOK (Dec. 21, 2011), https://www.facebook.com/notes/facebook-public-policy-europe/facebook-and-the-irish-data-protection-commission/288934714486394.

practices, not as the fulfillment of legal obligations. The same official told the BBC, "This is business as usual for us. Individuals raise concerns and take them to the regulatory authorities and we have a conversation with them."[334]

These friendly resolutions drew critics in both Ireland and the United States. According to Hawkes, some other European regulators objected to the outcome of the Facebook audit.[335] Much of the reaction to the FTC consent decree was likewise unimpressed, particularly in the heated world of technology blogs. A story on the website for *Wired Magazine* epitomized the common journalistic takeaway, calling it a "win for Facebook" and noting pointedly that the company was not required to admit fault.[336] The article began:

> Facebook is settling government charges it "deceived" users that their information would be kept private, although it was "repeatedly" shared with the public, the [FTC] announced Tuesday.
>
> The deal, which carries no financial penalties, demands that the social-networking site obtain "express consent" of their 850 million users before their information "is shared beyond the privacy settings they have established."[337]

These criticisms focused on the lack of a clear punishment for Facebook. But responsive regulation does not depend on punishments to achieve results, and Facebook's overall privacy performance has improved considerably since 2011.

Most significantly, Facebook has greatly expanded and formalized its privacy compliance functions. As part of this effort, every product manager now receives intensive privacy training and an internal privacy team carefully monitors the design of new features.[338] The creation of this "comprehensive privacy program" is very much in line with the recommendations of both the FTC and the ODPC. The involvement with product development epitomizes the FTC's "privacy by design" mantra.[339]

On its own initiative, without specific mandates from either regulator, Facebook also developed a new "privacy checkup tool," depicted in Figure 1, that periodically interrupts users when they log in and directs them to evaluate their

---

334. *Irish Privacy Watchdog Calls for Facebook Changes*, BBC NEWS (Mar. 8, 2012), http://www.bbc.com/news/technology-16289426.

335. *See* Mark Tighe, *Data Commissioner: I Was Not Too Soft on Facebook*, SUNDAY TIMES (UK) (Jan. 7, 2012), http://www.thesundaytimes.co.uk/sto/news/ireland/News/Irish_News/article853298.ece.

336. David Kravets, *FTC Slaps Facebook's Hand Over Privacy Deception*, WIRED (Nov. 29, 2011), http://www.wired.com/2011/11/ftc-slaps-facebook-privacy/.

337. *Id*. Technology bloggers reacted similarly to a more recent consent decree involving social network privacy, this one against Snapchat. One story began: "The [FTC] today effectively told technology companies: Go ahead and lie to consumers about your privacy protections, because even if you get caught, the most you'll have to do is apologize." Larson, *supra* note 4.

338. *See* Kashmir Hill, *The Guy Standing Between Facebook and Its Next Privacy Disaster*, FUSION (Feb. 4, 2015), http://fusion.net/story/41870/facebook-privacy-yul-kwon/.

339. *See supra* notes 267–271 and accompanying text.

settings before proceeding.[340] The tool,[341] pictured below, ensures that users reassess their own privacy—because not only might the architecture of Facebook change, but the individual user's preferences, habits, and personal relationships may alter over time.

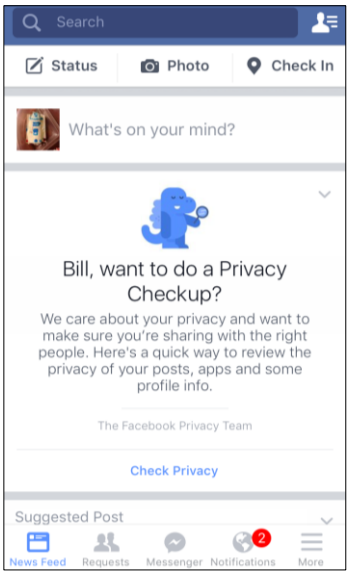

Figure 1: The Facebook Privacy Checkup Tool.

As a final indication of its increasing privacy consciousness, Facebook was the first large platform to require a search warrant for government investigators' requests for user data, rather than handing it over voluntarily.[343] This last position may not be one that government regulators value, but it is important to users.

The FTC and ODPC have continued to scrutinize Facebook since their 2011 investigations. In 2013, Facebook again altered its privacy policy.[344] U.S.

---

340. Jessica Guynn, *Facebook Rolling Out Privacy Checkup for Users*, USA Today (Sept. 4, 2014, 4:50 PM), http://www.usatoday.com/story/tech/2014/09/04/facebook-privacy-checkup-tool/15067743/.

341. In addition to prompting users periodically to complete the "checkup," Facebook also made the tool available from every user's toolbar. *See What's The Privacy Checkup and How Can I Find It?*, FACEBOOK: HELP CTR., https://www.facebook.com/help/443357099140264 (last visited Aug. 11, 2016).

343. *See generally Who Has Your Back? 2013*, ELECTRONIC FRONTIER FOUND., https://www.eff.org/who-has-your-back-2013 (last visited Oct. 10, 2016) (stating the organizations was "particularly impressed by the firm stance Facebook takes" on this issue). EFF issues annual reports about platforms' practices in response to government requests for user data. For the most recent (and links to earlier years' reports), see *Who Has Your Back? 2016*, ELECTRONIC FRONTIER FOUND., https://www.eff.org/who-has-your-back-2016 (last visited Oct. 16, 2016).

344. Vindu Goel, *Facebook to Update Privacy Policy, But Adjusting Settings is No Easier*, N.Y. TIMES: BITS BLOG (Aug. 29, 2013),

privacy advocacy groups sent a letter to the FTC (not quite a formal complaint, but with similar effect) arguing that the Commission should block the new rules.[345] With considerable publicity, the FTC let it be known that it was inquiring into whether the new policy violated the 2011 agreement.[346] This was part of the continued scrutiny envisioned in the consent decree, and in response, Facebook hastily explained that the new policy language was merely an attempt to clarify terms without changing them substantively—one of the goals embodied pervasively in both the FTC and ODPC actions.[347] Facebook eventually agreed to further changes in response to the regulators' concerns.[348]

More recently, the FTC and other regulators expressed concern about Facebook's activities in connection with its acquisition of the popular messaging platform WhatsApp. After the WhatsApp transaction in 2014, the FTC proactively—and publicly—wrote to Facebook and invoked both Section 5 and the consent decree, warning, "[I]f you choose to use data collected by WhatsApp in a manner that is materially inconsistent with the promises WhatsApp made at the time of collection, you must obtain consumers' affirmative consent before doing so."[349] In August 2016, the company announced that some personal data about WhatsApp customers, which had remained segregated from the rest of Facebook's data, would henceforth be shared.[350] Individual users received clear notice of the change from prompts in the app that required them to accept the new terms and allowed them to

---

http://bits.blogs.nytimes.com/2013/08/29/facebook-to-update-privacy-policy-but-adjusting-settings-is-no-easier/.

345. Vindu Goel, *Privacy Groups Ask F.T.C. to Block Facebook Policy Changes*, N.Y. TIMES: BITS BLOGS (Sept. 4, 2014), http://bits.blogs.nytimes.com/2013/09/04/privacy-groups-ask-f-t-c-to-block-facebook-policy-changes/.

346. *See* Vindu Goel and Edward Wyatt, *Facebook Privacy Change is Subject of F.T.C. Inquiry*, N.Y. TIMES (Sept. 11, 2013), http://www.nytimes.com/2013/09/12/technology/personaltech/ftc-looking-into-facebook-privacy-policy.html.

347. *See* Elizabeth Dwoskin, *FTC Probing Facebook's New Privacy Policy*, WALL ST. J. (Sept. 11, 2013), http://blogs.wsj.com/digits/2013/09/11/ftc-probing-facebooks-new-privacy-policy; Jeremy Kirk, *FTC: Facebook Privacy Policy Review Part of Regular Monitoring*, PC WORLD (Sept. 11, 2013, 7:35 PM), http://www.pcworld.com/article/2048603/ftc-facebook-privacy-policy-review-part-of-regular-monitoring.html.

348. *See* FEDERAL REGULATORY DIRECTORY 252 (17th ed. 2016).

349. Letter from Jessica L. Rich, Dir. of FTC Bureau of Consumer Prot., to Erin Egan, Chief Privacy Officer, Facebook Inc., and to Anne Hoge, Gen. Counsel, WhatsApp Inc. 3 (April 10, 2014), https://www.ftc.gov/system/files/documents/public_statements/297701/140410facebookwhatappltr.pdf ("Failure to take these steps could constitute a violation of Section 5 and/or the FTC's order against Facebook."); *see* Hayley Tsukayama, *FTC Warns Facebook, WhatsApp: Keep Your Privacy Promises*, WASH. POST (Apr. 10, 2014), https://www.washingtonpost.com/news/the-switch/wp/2014/04/10/ftc-warns-facebook-whatsapp-keep-your-privacy-promises/.

350. *Looking Ahead for WhatsApp*, WHATSAPP BLOG (Aug. 25, 2016), https://blog.whatsapp.com/10000627/Looking-ahead-for-WhatsApp.

opt out of the data disclosures.[351] The FTC has indicated that it will "carefully review" these changes.[352] That evaluation will boil down to deciding whether the opt-out procedures Facebook offered were close enough to the requirements of the 2011 consent decree and the FTC's 2014 call for "affirmative consent."

The new WhatsApp policy attracted considerable negative commentary.[353] But analysis of the changes will require a careful and nuanced balance: keeping individuals informed and in control of their personal data, while letting technology businesses evolve to offer innovative services and—not incidentally—make money. It is a close call. The conscientious rollout of these changes shows Facebook has come a long way from its privacy lurches prior to 2011. Collaborative engagement by regulators such as the FTC will be more likely to resolve the question than a simplistic *ex ante* rule or premature resort to punitive measures.

The Irish regulator similarly continued its use of collaborative techniques, before, during, and after its audit. Ever since the Dublin office opened, the ODPC and Facebook have both continuously emphasized their ongoing discussions about data protection practices. For example, the audit report highlighted a visit by then-Commissioner Hawkes to Facebook's U.S. headquarters in 2010.[354] Dixon, the current Commissioner, has stated more recently that her staff continues to be in weekly and sometimes daily contact with Facebook-Ireland.[355] As already noted, the ODPC conducted and published a 2012 follow-up audit assessing Facebook's progress in making improvements from the original audit.[356] And in 2016, Facebook made a number of changes in its configuration in response to "intense engagement" with the ODPC.[357]

In the abstract, such constant communication between the regulator and one of the most significant businesses under its authority could be seen as either excessively chummy or intensively meddlesome, depending on the circumstances and one's point of view. Here, it appears to be neither. Consistent with a responsive

---

351. *See How Do I Choose Not to Share My Account Information With Facebook to Improve My Facebook Ads and Products Experiences*?, WHATSAPP FAQ, https://www.whatsapp.com/faq/general/26000016 (last visited Oct. 31, 2016); *see also* Jules Polonetsky, *What's Up With WhatsApp and Facebook?*, LINKEDIN (Aug. 26, 2016), https://www.linkedin.com/pulse/whats-up-app-facebook-jules-polonetsky.

352. *See* Jeff John Roberts, *Facebook's Plan for WhatsApp to Get Close Look from FTC*, FORTUNE (Sept. 8, 2016), http://fortune.com/2016/09/08/whatsapp-facebook-ftc/.

353. *See, e.g.*, Dan Tynan, *WhatsApp Privacy Backlash: Facebook Angers Users by Harvesting Their Data*, GUARDIAN (Aug. 25, 2016), https://www.theguardian.com/technology/2016/aug/25/whatsapp-backlash-facebook-data-privacy-users (reporting on criticism of new Facebook and WhatsApp policies).

354. ODPC Facebook Audit, *supra* note 196, at 21.

355. Elaine Edwards, *Helen Dixon: Compliance on Data Protection Needs 'Constant Vigilance'*, IRISH TIMES (June 23, 2016), http://www.irishtimes.com/business/technology/helen-dixon-compliance-on-data-protection-needs-constant-vigilance-1.2694981.

356. *See supra* notes 327–28 and accompanying text.

357. *See* Weckler, *supra* note 330.

regulation model, Facebook kept regulators informed of its activities and they, in turn, helped the company stay within the boundaries of acceptable practices.

By friending the privacy regulators, Facebook availed itself of an authoritative source to consult about its legal obligations and protected itself from future penalties. If Facebook is in constant contact with a regulator and following its advice, how can that regulator then complain about Facebook's actions?

From a regulator's perspective, this outcome should be counted as a success.[358] Facebook has established the elaborate compliance monitoring the FTC wanted, and the consent decree gives the FTC continued leverage over Facebook until it expires in 2032. Facebook also continues to consult the ODPC about its obligations. After all, the regulators' goal is to improve data privacy practices, and Facebook is now obeying the law as the FTC and the ODPC interpret it. Moreover, responsive regulation achieves that goal in a way that keeps costs low both for the government and for the job-creating economic engine at Facebook.

The flexible outcomes of the two regulatory interventions, along with the continued consultation they established, also mean that privacy requirements on Facebook can continue to adapt as the technology, business methods, and cultural expectations of social media continue to change. A ruling that bluntly forbids an innovation might inadvertently prevent beneficial developments, such as the creation of the News Feed. Using responsive regulation, the FTC and ODPC can intervene to discuss new features and policies, offer alternate views, and promote privacy. Indeed, they can effectively require such changes, because Facebook is now subject to greater scrutiny in the middle portion of the regulatory pyramid.

Finally, the regulatory friendship allows Facebook to present itself to the world as privacy-conscious—but this good publicity comes at the price that it in fact maintain strong practices, or the resulting legal and reputational harm could be especially serious. In other words, by allowing their new friends at Facebook to brag about data practices, the regulators have helped maximize the business incentives for continued advancement of privacy.

V. LESSONS AND FUTURE STUDY

This final Part considers some of the lessons emerging from this study of responsive regulation in data privacy enforcement and the next steps toward understanding it. Section A discusses three lessons about the effectiveness of this regulatory strategy that we can learn from the implementation of the model in Ireland and the United States. Section B briefly notes some avenues for future study of this insufficiently theorized area.

358. Hawkes, who ran ODPC during the audit, certainly views it that way, as "an example of the use of enforcement powers that did not have to be backed up by more coercive measures." Hawkes, *supra* note 169, at 450–52 (assessing the ODPC Facebook Audit).

A. Lessons

1. Resources

Responsive regulation is often championed because it is cost-effective in comparison to command-and-control rulemaking and adversarial proceedings. While that is true, successful responsive regulation is not cheap either. In particular, successful privacy enforcement necessitates the resources to obtain technical expertise.[359]

According to Hawkes, completion of the ODPC Facebook Audit required three months of full-time work by one-third of his entire staff, which totaled only 22 people at the time.[360] That level of engagement could overwhelm an office that was a relatively sleepy operation for many years. Until recently, the ODPC's budget and staff were designed to oversee "leisure centres" and "letting agencies"[361]—not global technology behemoths like Facebook.[362]

To the derision of its critics, the ODPC has long been headquartered over a Centra convenience store in the small village of Portarlington in County Laois, 75 kilometers southwest of Dublin.[363] This unusual location resulted from a past government's short-lived decentralization policy that moved offices outside the capital,[364] but some viewed the backwater location as proof that the ODPC was not up to the job of policing technology multinationals.[365]

In 2015, the Irish government initiated a massive increase in the resources and status of the ODPC. That year, the budget grew from €1.8 million to €3.65 million, and the number of employees rose from 29 to 50.[366] In 2017, the ODPC's budget is slated for another enormous gain, to over €7.5 million (equivalent to over $8 million)—quadruple the 2014 budget.[367] The current government also made organizational changes to upgrade the ODPC's institutional status and bureaucratic

---

359. *See* BENNETT & RAAB, supra note 18, at 177.

360. *See* Tighe, *supra* note 335.

361. *See supra* notes 216–220 and accompanying text.

362. *See* Mirani, *supra* note 2.

363. *Id*. The town itself is economically depressed—in fact, it was featured in a six-episode sequence of a nationally broadcast television program called *Dirty Old Towns*, a "makeover" reality show about small villages that have "let themselves go." *See* DIRTY OLD TOWNS: PORTARLINGTON (2012), http://www.rte.ie/tv/dirtyoldtowns/Portarlington.html.

364. *See* Aoife Bannon, *The Tiny Irish Office That Takes on Facebook*, IRISH SUN (Oct. 22, 2015), http://www.thesun.ie/irishsol/homepage/irishfeatures/6704950/The-tiny-Irish-office-that-takes-on-Facebook.html.

365. Former commissioner Hawkes commented on this. *See* Burrell, *supra* note 2 ("There has been some sneering about where we are located, but the ground floor just happens to be occupied by a supermarket. It doesn't really alter anything.").

366. 2014 Annual Report, *supra* note 210, at 1.

367. Press Release, Office Data Prot. Comm'r, Data Protection Commissioner Welcomes Budget 2017 Increase in Funding (Oct. 13, 2016), https://www.dataprotection.ie/docs/13-10-2016-Data-Protection-Commissioner-welcomes-Budget-2017-increase-in-funding/1601.htm.

independence.[368] At the same time, it created a new position of a Minister for Data Protection within the Office of the Taoiseach (Ireland's prime minister) and filled it with a member of Ireland's parliament who also has responsibilities as a Minister of State for European Affairs.[369] Finally, the ODPC opened a second office in 2016—this one located on a landmark square in central Dublin.[370]

The enhanced budget and authority—and even the more dignified office space—should help the ODPC go about its job. The Irish regulators will continue to rely on their investigative and audit powers as central features of their responsive regulation approach, but these are labor-intensive undertakings. For Dixon to follow through on her stated plans to audit other large technology companies in a manner similar to the Facebook review, those enhancements will be important.[371]

It is more difficult to ascertain the resources devoted to privacy enforcement by U.S. regulators, because those functions are subsumed in larger agencies. According to documentation the FTC has submitted to Congress, it had 57 full-time staff positions related to its "Privacy and Identity Protection" function in the 2015 fiscal year, and a budget for these functions of just under $10 million.[372] Those numbers are a bit higher than the ODPC—but for a nation with a population some 80 times larger than Ireland's.

This comparison could be somewhat misleading for several reasons, First, the FTC is only one of multiple U.S. agencies enforcing privacy law. For a full accounting, one would need to add all the resources devoted to privacy regulation by state attorneys general and by numerous other federal agencies such as HHS, the Department of Education, and the U.S. financial regulatory bodies. To take just one

---

368. Press Release, Dep't Taoiseach, "Budget 2015 Signals a New Era for Data Protection in Ireland" - Murphy, http://www.taoiseach.gov.ie/eng/Taoiseach_and_Government/About_the_Ministers_of_State/Minister_of_State_for_European_Affairs_Data_Protection_and_EU_Digital_Single_Market/MoS_Murphy_s_Press_Releases/%E2%80%9CBudget_2015_Signals_a_New_Era_for_Data_Protection_in_Ireland%E2%80%9D_-_Murphy.html (last visited Oct. 10, 2016) (upgrading ODPC to a separate Office of the State).

369. *See* Karin Lillington, *Data Protection Must Be Front and Centre in Information Age*, IRISH TIMES (Feb. 5, 2015), http://www.irishtimes.com/business/technology/data-protection-must-be-front-and-centre-in-information-age-1.2091272 (discussing the appointment of Dara Murphy as the first Minister for Data Protection, not only in Ireland, but in Europe).

370. *See* Press Release, Dep't Taoiseach, An Taoiseach and Minister Murphy Announce New Dublin Premises for the Office of the Data Protection Commissioner, http://www.taoiseach.gov.ie/eng/News/Taoiseach's_Press_Releases/An_Taoiseach_and_Minister_Murphy_announce_new_Dublin_premises_for_the_Office_of_the_Data_Protection_Commissioner_.html (last visited Oct. 31, 2016). The Portarlington office will remain in operation and technically continue as the headquarters. *Id.*; *Contacting Us*, DATA PROTECTION COMMISSIONER, https://www.dataprotection.ie/docs/Contact-us/b/11.htm (last visited Oct. 23, 2016).

371. *See supra* note 330.

372. *See* FTC, FISCAL YEAR 2016 CONGRESSIONAL BUDGET JUSTIFICATION 129–31 (2015), https://www.ftc.gov/system/files/documents/reports/fy-2016-congressional-budget-justification/2016-cbj.pdf.

example, the division of HHS most directly responsible for enforcement of HIPAA had a budget in Fiscal Year 2015 of just under $6.8 million,[373] which by itself approaches the ODPC's entire budget. In addition, remember that the ODPC must oversee, not only every industry, but also the public sector. Finally, while the ODPC is a free-standing entity, privacy regulators at larger agencies such as the FTC and HHS can rely on other less specialized staff in their agencies (such as lawyers, office technology, or meeting planning), so counting only the staff fully devoted to privacy may understate the available support. Even with all that, it still seems unlikely that the combined budgets of U.S. privacy regulators would add up to $640 million, as would be necessary to have roughly the same spending per capita as Ireland will have next year.

Setting aside the comparison, it is probable that funding for both U.S. and Irish privacy regulators is too limited. Privacy regulators' staff sizes differ widely, but both the ODPC and the FTC are much smaller than several countries' DPAs that have over a hundred employees, including those in France, Spain, and the United Kingdom.[374]

By the nature of government, regulators almost always operate under resource constraints. Nevertheless, modest budgets and staffing surely force these agencies to decline regulatory interventions that would be prudent. That does not necessarily mean the extra money should be spent on adversarial enforcement. But communication with regulated entities, development of educational materials and guidance, and preliminary investigation all cost money, too. This is an area for further improvement in both countries.

2. Penalties

As described earlier, the classic theory of responsive regulation requires a "benign big gun" that remains behind the door, loaded, and well oiled.[375] We have established that the gun in regulatory friending is benign, but is it sufficiently loaded and oiled? Do the penalties available at the top of the regulatory pyramid create sufficient leverage when negotiations occur at lower levels of that pyramid?

Perhaps the most obvious penalty—and the one that critics of the collaborative approach taken by the FTC and ODPC seem to expect[376]—would be a monetary fine. Even had they wished to impose a fine on Facebook in the first instance, neither the ODPC nor the FTC had the power to do so at the time.

---

373. DEP'T HEALTH & HUMAN SERVS., OFFICE CIVIL RIGHTS, FISCAL YEAR 2016 CONGRESSIONAL BUDGET JUSTIFICATION 27–29 (Feb. 2, 2015), http://www.hhs.gov/sites/default/files/budget/office-of-civil-rights-budget-justification-2016.pdf.

374. *See* David Wright, *Enforcing Privacy*, *in* ENFORCING PRIVACY, *supra* note 15 at 13, 29–30 (listing the number of employees working for various data protection authorities around the world as of 2013).

375. *See supra* notes 160–166 and accompanying text.

376. *See supra* notes 2–4 and accompanying text.

Under the current Data Protection Act in Ireland, a financial penalty is likely only in the rare prosecutions that reach court, and even there the maximum sums are modest, typically just a few thousand euros.[377] The GDPR will usher in a dramatically different penalty structure, which will automatically take effect in Ireland in 2018. Its graduated administrative fines are complicated, but in the most serious cases could amount to 4% of a company's global annual turnover—that is, revenue.[378] In preparation for its initial public offering, Facebook reported gross revenue in 2011 of $3.7 billion.[379] Thus, if the ODPC had been able to conduct its 2011 Facebook investigation under the new 2018 rules, it theoretically could have fined the company up to $148 million if it uncovered very serious privacy flaws.

Certainly, a fine of this magnitude would be a potent regulatory weapon. In fact, the maximum fine is so large that a threat to impose it might not be terribly credible.[380] Under the graduated penalty structure, the ODPC would also have the option of charging an amount that is considerably lower than 4% of revenue, but still significant.

The FTC cannot fine an entity either, at least not when relying solely on its powers under Section 5. As noted previously, the FTC can parlay a consent decree entered for a first offense into fines for subsequent infractions, as it did against Google.[381] The FTC also enjoys the authority to fine companies for violations of other statutes such as COPPA, and it has exercised this power frequently to extract civil penalties in settlements.[382] A few U.S. regulators can impose very large fines. The California Attorney General recently settled a consumer-protection suit with Comcast, which had carelessly published telephone numbers of customers who had paid to have unlisted numbers.[383] The price tag was a $25 million civil penalty plus nearly $8 million in restitution.[384] In the foreseeable future, however, the FTC will not have traditional fining authority in the bulk of its consumer protection jurisdiction, except over companies already covered by consent decrees.

---

377. *See supra* note 228–235 and accompanying text.

378. *See* GDPR, *supra* note 13, at art. 83.

379. *See* Tomio Geron, *Facebook's $5 Billion IPO Filing: $3.7 Billion in 2011 Revenue*, FORBES (Feb. 1, 2012), www.forbes.com/sites/tomiogeron/2012/02/01/facebooks-5-billion-ipo-filing-3-7-billion-in-2011-revenue/.

380. *See supra* note 163 and accompanying text.

381. *See supra* notes 259–64 and accompanying text.

382. *See, e.g.*, United States v. Yelp, Inc., Case No. 3:14-CV-04163 (N.D. Cal. Sept. 17, 2014) (order) ($450,000 penalty); United States v. Artist Arena, LLC, Case No. 112-CV-07386 (S.D.N.Y. Oct. 4, 2012) (Order) (one-million-dollar penalty). That said, the FTC also uses responsive regulation under COPPA. *See* HOOFNAGLE, *supra* note 15, at 206–07 (describing use of safe harbor programs, an enforcement approach under COPPA that adheres to the responsive regulation model).

383. *See* California v. Comcast Cable Commc'ns Mgmt., LLC, No. 15786197 (Cal. Super. Ct. Sept. 17, 2015) *in* MCGEVERAN, *supra* note 23, at 248.

384. *Id*. at 254–55. Based on the Attorney General's allegations about the number of violations and the maximum possible statutory penalty. In the event of a fully favorable verdict, Comcast might have been liable for over $262 million. *See* MCGEVERAN, *supra* note 23, at 255.

The FTC does have some powers fairly high up the pyramid that can help cajole companies into compliance. Even the initiation of an FTC investigation is viewed by many regulated entities as a serious problem. The imposition of ongoing oversight in consent decrees is even more significant. One U.S. corporate privacy official interviewed by Bamberger and Mulligan went so far as to call the possibility of operating under a decree a "Three-Mile Island scenario" that motivated top executives in the firm to take privacy and security issues seriously.[385] So, while the FTC's regulatory pyramid may not rise to quite as high a peak as those of some other American regulators, and certainly not to where E.U. regulators will reach under the GDPR, the FTC's top-of-the-pyramid penalties still manage to alarm and motivate corporate privacy managers and their bosses.

That said, the FTC would probably be able to act more effectively, even as a friendly regulator, if it had the power to levy fines under Section 5. A regulator does not need to impose its most severe punishments often, or perhaps at all, to influence all other cases.[386] The risk of being subjected to an investigation or a consent decree for poor data-handling practices, while meaningful, is presumably not as potent a disincentive as a direct financial penalty. If the agency retained the money raised by fines, it could also use them to provide some of the necessary resources identified in Section III.A.1, above.

3. Accountability

Behind much of the criticism of friendly privacy regulation is a suspicion, stated or implied, that regulators might be captured by companies. In order to maintain accountability, responsive regulation must be responsive not only to companies, but also to the public, advocacy groups, the media, and legislators.

In Ireland, several formal mechanisms foster that accountability and help prevent the ODPC from entering an overly cozy friendship with regulated entities. First, as mentioned previously, the ODPC acts on every complaint it receives.[387] Admittedly, a fully captured agency could give short shrift to many complaints. But a formal complaint mechanism still provides an opportunity for ordinary citizens to disrupt any capture dynamic. The ODPC's annual reporting of statistics about the disposition of complaints further enhances this accountability function.[388] Besides, capture is possible no matter what punishments agencies can or do impose—transparent procedures and strong ethics rules are more effective prophylactics against capture, regardless of the regulatory approach adopted.[389]

Not only does the complaint procedure itself enhance accountability, but people dissatisfied with the ODPC's initial response can challenge it in court. This is exactly what Schrems did in his Safe Harbor case objecting to the ODPC's

---

385. Bamberger & Mulligan, *supra* note 16, at 274.

386. *See* AYRES & BRAITHWAITE, *supra* note 130, at 36–37; GUNNINGHAM & GRABOSKY, *supra* note 134, at 396–97, 396 nn.50–51.

387. *See supra* notes 204–05 and accompanying text.

388. *See supra* note 210 and accompanying text.

389. *See generally* DANIEL CARPENTER & DAVID A. MOSS, EDS., PREVENTING REGULATORY CAPTURE: SPECIAL INTEREST INFLUENCE AND HOW TO LIMIT IT (2013).

dispositions of some of his complaints against Facebook.[390] The Data Protection Act instructs the ODPC to issue formal decisions even when it elects to take no further action.[391] While the Irish courts adhere to a doctrine of "curial deference" with regard to administrative agencies, they do serve as a check against actions that are arbitrary, unduly credulous toward industry, or contrary to the judicial understanding of the law, as demonstrated, again, by the *Schrems* Safe Harbor litigation.[392] Serious challenges may then be referred from Irish courts to E.U. courts, as happened in *Schrems*.[393] Possible intervention by E.U. courts helps prevent a "race to the bottom" on data protection by Irish institutions, whether regulatory or judicial.[394] Too great a departure from established E.U. data protection norms can and will be overturned.

Nor is judicial review the only external check on the ODPC's enforcement choices.[395] Article 29 of the Data Protection Directive established an advisory body composed of representatives from each nation's data protection regulatory agency and from the European Commission.[396] The so-called "Article 29 Working Party" issues detailed opinions interpreting the requirements of E.U. data protection law.[397] While these determinations are only advisory, they are highly influential. National and E.U. courts cite them as persuasive authority and there is strong institutional

---

390. *See* Case C-362/14, Schrems v. Data Prot. Comm'r, 2015 EUR-Lex CELEX LEXIS 62014CJ0362 (Oct. 6, 2015).

391. *See* Irish Data Protection Act, *supra* note 51, § 11(a)(2).

392. *See* Patrick O'Reilly, *The Doctrine of Curial Deference in Ireland*, 7 JUD. STUDS. INST. J. 197, 197 (2007), http://www.jsijournal.ie/html/Volume%207%20No.%202/2007%5B2%5D_O'Reilly_Curial%20Deference%20in%20Ireland.pdf (describing curial defense as judicial restraint when reviewing decisions of independent regulatory "expert" bodies).

393. The ODPC can also seek rulings from the Court of Justice directly, and the ODPC recently did so in response to yet another Schrems complaint, challenging the validity of model contract clauses to permit cross-border data transfers in the wake of the earlier Safe Harbor decision. *See* Alexander J. Martin, *Irish Data Cops Kick Max Schrems' Latest Facebook Complaint Up to EU Court*, REGISTER (May 25, 2016), http://www.theregister.co.uk/2016/05/25/ireland_data_protection_commissioner_asks_eu_decision_max_schrems_complaint/.

394. *See* Cass R. Sunstein, *Constitutionalism After the New Deal*, 101 HARV. L. REV. 421 (1987) (discussing the importance of checks and balances in regulatory authorities); *cf.* Richard L. Revesz, *Rehabilitating Interstate Competition: Rethinking the "Race-to-the-Bottom" Rationale for Federal Environmental Regulation*, 67 N.Y.U. L. REV. 1210 (1992).

395. *See* Francesca Bignami, *Mixed Administration in the European Data Protection Directive: The Regulation of International Data Transfers* 1 RIVISTA TRIMESTRALE DI DIRITTO PUBBLICO 31 (2004), http://ssrn.com/abstract=2232325 (analyzing "mixed administration" between national and E.U.-level authorities in the enforcement of the Directive's limits on cross-border data transfers).

396. E.U. Data Protection Directive, *supra* note 44, art. 29.

397. *See Article 29 Working Party*, EUR. COMMISSION: JUSTICE, http://ec.europa.eu/justice/data-protection/article-29/index_en.htm (last visited Aug. 5, 2016).

pressure for national regulators not to stray too far from the consensus of their peers.[398]

The GDPR will introduce additional restraints. The ODPC would continue to function as the "lead supervisory authority" with jurisdiction over companies that have their "main establishment" in Ireland.[399] Consequently, the ODPC will maintain significant influence over data protection enforcement against Facebook, Google, Apple, and all the other technology giants who have their largest European presence on Irish soil. This lead supervisory authority is not, however, exclusive power, as was envisioned in some earlier proposals for a "one stop shop" regulatory structure in the EU.[400] Rather, the GDPR sets up a consultation process for a primary regulator like the ODPC to confer with data protection regulators in other countries where people were affected by a challenged data-handling practice.[401] A newly created European Data Protection Board will resolve disagreements between national regulators about the regulatory approach taken.[402]

It remains to be seen, in 2018 and beyond, exactly how the E.U. will structure this new Board and the consultation process. These conformity mechanisms must try to balance the sovereign interests of E.U. member states with the Union's objective of harmonizing law across the integrated European market.[403] The prospects for responsive regulation within that structure will be an important area for future study. If E.U. member states meddle with one another, national regulators like the ODPC could find themselves hindered from using more collaborative techniques. If handled with respect for national choices of regulatory style, however, these additional accountability mechanisms may simply provide further assurance that friendly regulation does not become crony regulation.

The FTC is not subject to many formal mechanisms of this nature. The Commission is not required to act on complaints, and citizens cannot challenge regulatory inaction in court, or elsewhere. Public comments on consent decrees seldom have any impact.[404] Greater institutional accountability might be desirable

---

398. *See* CAREY, *supra* note 56, at 56 (describing the influence of the Article 29 Working Party on Irish data protection law); KUNER, *supra* note 22, at 9–10 ("Pronouncements of the Working Party can have significant impact on the decisions of national courts and DPAs.").

399. *See* GDPR, *supra* note 13, art. 4, §16 (defining a company's "main establishment" as "the place of its central administration in the [European] Union"); *id*. art. 56 (designating the regulator in a company's "main establishment" as the "lead supervisory authority" with primary jurisdiction over the company's compliance with data protection law).

400. *See, e.g.*, 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 (COM 2012) 11, 32 ¶97.

401. GDPR, *supra* note 13, arts. 60–62.

402. *Id*. arts. 60, 63–66, 68 (creating the Board and specifying resolution and consistency mechanisms for disagreements between national DPAs).

403. *See supra* notes 39–40 and accompanying text.

404. *See supra* note 257 and accompanying text.

to reduce the risk of capture, empower individuals, and increase public acceptance of the FTC's regulatory choices.

One accountability mechanism that is stronger in the United States than in Ireland is a comparatively robust privacy advocacy community.[405] Nongovernmental organizations such as the Electronic Privacy Information Center,[406] the Electronic Frontier Foundation,[407] the Center for Democracy and Technology,[408] and many others serve as watchdogs and gadflies to prevent inappropriate behavior by regulatory agencies. When these organizations call on regulators to act, they can also mobilize press coverage, questions from sympathetic members of Congress, and grassroots pressure from their members.[409]

Privacy advocacy in Ireland is more limited. Digital Rights Ireland[410] has made considerable inroads, including a successful E.U. court case to overturn a data retention directive that it argued compromised citizen privacy in relation to law enforcement.[411] Groups from other E.U. countries (including Schrems's organization) also intercede in Ireland.[412] Even so, scrutiny of the ODPC by NGOs and media may be somewhat less intense than what the FTC receives. It might also be less important in light of the formal accountability mechanisms in Irish and E.U. law that are missing in the United States. Perhaps such groups in both countries could be further strengthened by means that Ayres and Braithwaite call "tripartism," where external watchdogs have access to information held by regulators, increasing their power to prevent capture or collusion between government and industry.[413]

B. Further Study

Privacy scholars have begun to pay more attention to the actual practices of privacy regulation "on the ground." Yet the map of that space is far from

405. *See* COLIN J. BENNETT, THE PRIVACY ADVOCATES (2010) (discussing the role of independent advocates to spur government action against problematic data practices).

406. ELECTRONIC PRIVACY INFO. CTR., www.epic.org (last visited Sept. 21, 2016).

407. ELECTRONIC FRONTIER FOUNDATION, www.eff.org (last visited Sept. 21, 2016).

408. CTR. DEMOCRACY & TECH., www.cdt.org (last visited Sept. 21, 2016).

409. *See* BENNETT, *supra* note 405, at 328; *see also* GUNNINGHAM & GRABOSKY, *supra* note 134, at 94–106 (making similar points about environmental public interest groups).

410. DIGITAL RIGHTS IRELAND, https://www.digitalrights.ie/ (last visited Sept. 21, 2016).

411. *See* Case 293/12, Digital Rights Ireland Ltd. v. Minister for Commc'ns, Marine & Nat. Res. (Apr. 8, 2014), http://curia.europa.eu/juris/document/document.jsf?docid=150642&doclang=EN.

412. *See, e.g.*, EDRI, https://edri.org/about (last visited Sept. 21, 2016) (describing the structure of pan-EU coalition of digital privacy advocacy groups).

413. *See* AYRES & BRAITHWAITE, *supra* note 130, at 54–100.

complete.[414] Research such as Bennett's groundbreaking work;[415] Bignami's empirical study of data protection regulatory styles in four European countries;[416] or Bamberger and Mulligan's comprehensive examination of corporate behavior[417] blazed the trail toward the study of real practices rather than just formal law. Recent scholarly examinations of the institutional role of particular regulatory agencies in the overall enforcement scheme add important details to the map.[418]

This Article has added an analysis of responsive regulation as an effective privacy enforcement tool, and a focus on the especially important practices of Ireland's DPA. But there is much more to be done to expand the examination here across several dimensions. One important path to continue exploring is methodological. Observation and interviews with regulatory officials would contribute greatly to understanding the motivations and rationales for the choices they make.[419] This form of observational case study is very well established in the responsive regulation literature outside of the privacy context.[420]

Another fruitful trail would be an extension of the inquiry to other regulatory agencies and other statutes. Why does the ODPC make different choices of regulatory approaches than some other European regulators, and how do the results of these different approaches compare? Among U.S. regulators, this Article has focused on the FTC exercising its Section 5 authority. Sectoral U.S. privacy regulators such as HHS and the Department of Education's Office of Civil Rights broadly emulate the responsive approach taken by the FTC. And the FTC itself embraces responsive regulation techniques under COPPA, which is a data protection statute. Likewise, Jane Winn has described the Red Flags Rule, developed jointly by the FTC and financial regulatory agencies to reduce financial identity theft risk, as an example of new governance techniques.[421]

---

414. *Cf.* Donald Clarke, *'Nothing But Wind?' The Past and Future of Comparative Corporate Governance*, 59 AM. J. COMP. L. 75, 94 (2010) (similarly arguing that comparative corporate governance scholarship "would benefit from a stronger focus on the institutional environment for corporate governance. This means comparing not just rules, no matter how well selected, but also the various institutions that exist to make the rules meaningful.").

415. *See* BENNETT & RAAB, *supra* note 18; BENNETT, *supra* note 405; BENNETT, *supra* note 18.

416. *See* Bignami, *supra* note 15

417. *See* BAMBERGER & MULLIGAN, *supra* note 16; Bamberger & Mulligan, *supra* note 16.

418. *See, e.g.*, HOOFNAGLE, *supra* note 15; Citron, *supra* note 15; Solove & Hartzog, *supra* note 15.

419. For examples of work about privacy regulation employing interview-based methodology, see BAMBERGER & MULLIGAN, *supra* note 16; BENNETT & RAAB, *supra* note 18; Hirsch, *supra* note 15.

420. The works collected in REGULATORY ENCOUNTERS, *supra* note 6, provide numerous examples. *See also* BRAITHWAITE, *supra* note 151, at 17–19 (describing interview-based study of Australian nursing home regulation); Schwarcz, *supra* note 155, at 735 n.* (describing extensive use of interviews in detailed examination of United Kingdom's Financial Ombudsman Service and insurance regulators in several U.S. states).

421. Jane K. Winn, *Are 'Better' Security Breach Notification Laws Possible?*, 24 BERKELEY TECH. L.J. 1133, 1163–64 (2009).

Finally, it is not certain that responsive regulation is equally effective in all aspects of data privacy enforcement: do lessons shaped by the social media case study in this Article extend fully to areas such as regulation of data breaches or de-identification of personal information?

These questions help to shape a research agenda for this author and other scholars that will both critique existing regulatory models and contribute to their improvement.

CONCLUSION

Adversarial combat is not the only effective mode of regulation. New governance scholars have explained the benefits of models like responsive regulation. Techniques of collaboration, flexibility, and the carefully graduated penalties of the regulatory pyramid work well for enforcement of privacy and data protection law. They help regulators to encourage companies to improve their practices continually, retain the flexibility to deal with changing technology, and discharge their oversight duties cost-effectively—while maintaining the well-oiled "shotgun behind the door" as an incentive for companies to comply.

In addition, when regulators under different legal regimes share this cooperative regulatory approach, it bridges gaps between them and can enable companies to develop common global strategies based on best practices that comply with legal requirements in disparate jurisdictions. This makes the theoretically sharp differences between countries less significant in practice.

There is room for improvement of responsive privacy regulation, and many topics require further exploration. Nevertheless, the case study examined here—the regulatory styles used in the U.S. and Ireland, particularly with regard to their parallel investigations of Facebook—suggest that "regulatory friending" works effectively in the privacy context. Collaboration gives companies more clarity about their compliance obligations and minimizes their risk of being surprised by an adversarial regulatory action. Meanwhile, regulators can improve real-world data practices efficiently, flexibly, and cooperatively.