THE VALUE OF MODEST PRIVACY PROTECTIONS IN A HYPER SOCIAL WORLD

WOODROW HARTZOG*

INTRODUCTION

Two of the greatest modern challenges to protecting personal information are determining how to protect information that is already known by many and how to create an adequate remedy for privacy harms that are opaque, remote, or cumulative. Both of these challenges are front and center for those who seek to protect socially shared information. Social media and wearable communication technologies like Google Glass present vexing questions about whether information that is known by many can ever be "private," what the privacy harm might be from this information's misuse, and how to remedy such harms in balance with competing values such as free speech, transparency, and security. Some law and policy makers have responded to the challenge of protecting privacy in an era of massive self-disclosure with relatively modest, piecemeal protections.

For example, rather than refrain from collecting or using personal

*Assistant Professor, Samford University's Cumberland School of Law; Affiliate Scholar, Center for Internet and Society at Stanford Law School. The author would like to thank Alvaro Bedoya, Paula Bruening, Ryan Calo, Brannon Denning, Michael Hintze, Paul Ohm, Rob Sherman, Harry Surden, and the participants of The New Frontiers of Privacy Harm Event hosted by the Silicon Flatirons Center.

information, some companies are required only to provide notice of their practices.[1] Instead of being prohibited from using information posted on social media accounts in hiring decisions, some companies must only refrain from asking for access to applicant's social media profiles or login credentials.[2] As an alternative to problematic personal information being purged entirely from a database, some companies need only make that information inaccessible to other Internet users.[3]

The true value of these protections is not always appreciated. Privacy advocates often find relatively weak or incomplete privacy protections to be "watered down," while critics of privacy regulations point to the failure of complete protection as evidence that a particular law is unjustified. For example, many criticized California's SB 568, known as the "online eraser law."[4] Among other things, from 2015 on this law gives residents under 18 a limited right to delete personal information that they, as registered users of sites and networks, posted online or on a mobile app. SB 568 was criticized by some for being overprotective and by others for not being protective enough. This variance in criticism is emblematic of many modern privacy debates.[5]

Some privacy advocates claimed that the law didn't go far enough because it is full of exceptions like excluding re-posts from protection and, as a result, is too limited in scope to properly protect teenagers.[6]

1. *See, e.g.*, CAL. BUS. & PROF. CODE § 22581(a) (West, Westlaw through 2013 portion of 2013-2014 Legis. Sess.) (effective Jan. 1, 2015).

2. ARK. CODE ANN. § 11-2-124 (2013); CAL. LAB. § 980 (2014); COLO. REV. STAT. ANN. § 8-2-127 (2013); 820 ILL. COMP. STAT. ANN. 55/10 (2014); MD. CODE ANN., LAB. & EMPL. § 3-712 (2013); MICH. COMP. LAWS ANN. § 37.273 (2013); NEV. REV. STAT. § 613.135 (2013); N.J. STAT. ANN. § 34:6B-6 (2013); N.M. STAT. ANN. § 50-4-34 (2013); 2013 Or. Laws ch. 204; UTAH CODE ANN. § 34-48-201 (2013); WASH. REV. CODE ANN. § 49.44.200 (2013).

3. *See* CAL. BUS. & PROF. CODE § 22581(d).

4. *See* Eric Goldman, *California's New 'Online Eraser' Law Should be Erased*, FORBES (Sept. 24, 2013, 1:35 PM), http://www.forbes.com/sites/ericgoldman/2013/09/24/californias-new-online-eraser-law-should-be-erased/; Gregory Ferenstein, *On California's Bizarre Internet Eraser Law for Teenagers*, TECHCRUNCH (Sept. 24, 2013), http://techcrunch.com/2013/09/24/on-californias-bizarre-internet-eraser-law-for-teenagers/; *see also* Kurtis Alexander & Vivian Ho, *New Law Lets Teens Delete Digital Skeletons*, SFGATE (Sept. 24, 2013, 9:47 AM), http://www.sfgate.com/bayarea/article/New-law-lets-teens-delete-digital-skeletons-4837309.php; Peter Weber, *Could a Social Media Eraser Law Save an Over-Sharing Generation?*, THE WEEK (Sept. 20, 2013), http://theweek.com/article/index/249988/could-a-social-media-eraser-law-save-an-over-sharing-generation; Damon Brown, *Is California's social media 'eraser' law a losing battle?*, AL JAZEERA (Nov. 8, 2013, 5:00 AM), http://america.aljazeera.com/articles/2013/11/8/is-california-s-socialmediaeraserlawalosingbattle.html.

5. *See* Eric Goldman, *How California's New 'Do-Not-Track' Law Will Hurt Consumers*, FORBES (Oct. 9, 2013, 1:54 PM), http://www.forbes.com/sites/ericgoldman/2013/10/09/how-californias-new-do-not-track-law-will-hurt-consumers. *See generally,* Paul Ohm, *Good Enough Privacy*, 2008 U. CHI. LEGAL F. 1, 63 (2008).

6. *See* Goldman, *supra* note 4; Ryan Garcia, *We Don't Care About Privacy, But We Care About the Children*, SOMELAW THOUGHTS (July 9, 2013, 8:13 AM),

Advocates of commercial and technological innovation raised the same objection to argue that the law wasn't effective enough to justify its existence.[7] The result of this and similar debates is that the value of modest privacy protections for social shared information is often overlooked. The limitations in the eraser law represent deference to free speech principles while giving users the option of erasing heaps of problematic disclosures that no one found interesting enough to share.

The marginalization of perceived "weak" protections for socially shared information is misguided. Criticisms of such protections are often based upon a misperception that it is futile or unnecessary to protect information that is shared with other people. There are many different kinds of privacy harm that require some legal response yet do not need vigorous, "lockdown" legal protections. Indeed, in many instances such protection would be counter-productive in preserving privacy.

This essay argues that modest and incremental privacy protections might be one of the most effective ways to protect semi-private information while balancing it with competing values. The cumulative effect of modest protections can be quite robust. The purpose of this essay is to explore the trend of providing modest protection for semi-private information and highlight the value of this modesty as one part of a holistic legal response to the panoply of modern privacy harms.

The first part of this essay explores this new wave of modest privacy protections. It organizes them into two main categories: protections with porous coverage and protections that provide weak or indirect remedies. The second part of this essay explores the underestimated value of modest privacy protections. The digital age requires a more granular, diverse, and contextual conceptualization of privacy. Modest protections can fulfill this need by filling out the spectrum of available remedies to reach information that has been disclosed to some but not all. Modest privacy protections are typically more politically palatable than robust protections. Because they are incremental, modest protections are also adaptable to new technologies and evolving norms. Additionally, by embracing modest protections, privacy regulation can be better conceptual-

http://somelaw.wordpress.com/2013/07/09/we-dont-care-about-privacy-but-we-care-about-the-children/; Charley Lozada & Jeff Neuburger, *New California Law Impacts Use of Information from Minors, Offers Right to Delete*, NEW MEDIA & TECH. L. BLOG (Nov. 19, 2013), http://newmedialaw.proskauer.com/2013/10/02/new-california-law-impacts-use-of-information-from-minors-right-to-delete-and-other-provisions-likely-to-have-nationwide-effect/; Katy Waldman, *California's Internet Eraser Law: Nice Idea, but it Won't Work*, SLATE (Sept. 25, 2013, 3:07 PM), http://www.slate.com/blogs/xx_factor/2013/09/25/sb_568_california_digital_eraser_law_for_minors_is_unlikely_to_work.html.

7. Goldman, *supra* note 4; *see also* Somini Sengupta, *Sharing, With a Safety Net*, N.Y. TIMES (Sept. 19, 2013), http://www.nytimes.com/2013/09/20/technology/bill-provides-reset-button-for-youngsters-online-posts.html?_r=0.

ized as an ongoing process rather than a static line in the sand.

While modest privacy protections are certainly no substitute for robust protections in many contexts, they can be valuable in contexts where strong protections are unsuitable. For example, modest privacy protections are useful when harms exist yet are opaque, novel, cumulative, or remote. Instead of seeking to rigorously protect every kind of traditionally defined "private" information, this essay argues that the law should instead strive to protect more kinds of non-secret personal information less robustly. Lower and indirect levels of protection for some categories of information based on social norms as well as individual preferences are more politically feasible and often reflect a balance between privacy and competing interests. Design-based protections, such as data security and certain aspects of "privacy by design," are comparatively modest in that they are indirect. Focusing on design might be the most effective way to protect against privacy harms that are not concrete, direct, or severe.

I. A NEW WAVE OF MODEST PRIVACY PROTECTIONS

In a sense, all U.S. privacy law is comparatively modest because it is sectoral in nature. There is no omnibus privacy law in the United States.[8] For example, the Family Educational Rights and Privacy Act (FERPA) only protects the privacy of school records, the Health Insurance Portability and Accountability Act (HIPAA) only protects the privacy of medical records, the Video Privacy Protection Act (VPPA) protects the privacy of video rental information, and so on.[9] State privacy protections often explicitly only protect residents.[10] To the extent these laws are criticized as weak or incomplete, this essay joins the body of literature that sees value in an incremental and sectoral approach to privacy.[11]

8. Paul M. Schwartz, *Preemption and Privacy*, 118 YALE L.J. 902 (2009).

9. *See* Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g (2011); Health Insurance Portability and Accountability Act, Pub. L. No. 104-191, 110 Stat. 1936 (1996) (codified in scattered sections of 26, 29, and 42 U.S.C.); Video Privacy Protection Act, 18 U.S.C. § 2710 (2011).

10. *See, e.g.*, CAL. BUS. & PROF. CODE § 22580(d) (West, Westlaw through 2013 portion of 2013-2014 Legis. Sess.) (effective Jan. 1, 2015) (defining "minor," for purposes of California's online eraser law, as "a natural person under 18 years of age who resides in the state").

11. Margot E. Kaminski, *Drone Federalism: Civilian Drones and the Things They Carry*, 4 CAL. L. REV. CIRCUIT 57, 59 (2013) ("Like all laws governing videos by private actors, drone surveillance laws will exist between a privacy floor and a First Amendment ceiling. For now, I argue, this complex space of privacy regulation is best left to the states."); Schwartz, *Preemption and Privacy, supra* note 8. *But see* Patricia L. Bellia, *Federalization in Information Privacy Law*, 118 YALE L.J. 868, 871 (2009) ("the case for federal regulation of data privacy is stronger than Schwartz suggests, even when federal regulation would preempt state law in favor of a unitary federal standard. In addition, I view carefully crafted minimum priva-

But there are others kinds of modesty that are less frequently valued by privacy advocates, in particular, protections that don't apply to the full range of bad actors or problematic practices and protections that fail to directly prohibit problematic activities. Critics often perceive these types as inadequate because they either seemingly let too many problematic activities slip through the cracks or they only aim to reduce the likelihood of harm rather than completely prevent it. But probabilistic protections can serve as bedrock principles for self-regulatory and regulatory schemes. For example, design-based protections like those found in the Fair Information Practice Principles are indirect protections meant to reduce the probability of privacy harm rather than directly prohibit it.[12]

These critics often appropriately point out the shortcomings of modern privacy law.[13] The limited coverage of our electronic surveillance regime is outdated and problematic because it does not cover many different kinds of communications that society has come to expect as private, such as communications stored in the cloud.[14] The Fair Credit Reporting Act (FCRA) could serve as the blueprint for the protection of massive dossiers of personal information held by organizations such as commercial data brokers, yet this important federal statute only applies to "consumer reporting agencies" that furnish "consumer reports."[15] When privacy protections become outdated or ineffective due to changing technologies and cultural assumptions, they should be modified accordingly.

But other privacy protections are desirable precisely because they are modest. These protections, which are the focus of this essay, often apply in the messy context of socially shared information, where privacy ideals and boundaries are difficult to discern or are in competition with other important values. For example, the disclosure tort is rightfully lim-

cy standards that cut across sectoral lines as unproblematic, so long as such standards permit stronger sector-specific approaches."); Elizabeth D. De Armond, *A Dearth of Remedies*, 113 PENN ST. L. REV. 1, 4 (2008) ("Congress's interest in privacy issues has grown over the last four decades, but effective protection has shrunk.").

12. Robert Gellman, *Fair Information Practices: A Basic History* (Mar. 18, 2014), http://bobgellman.com/rg-docs/rg-FIPShistory.pdf; *see also* FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE (2012), *available at* http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

13. *See generally* 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); Neil M. Richards & Daniel J. Solove, *Prosser's Privacy Law: A Mixed Legacy*, 98 CAL. L. REV. 1887 (2010).

14. *See* Mark Stanley, *Day of Action to Demand ECPA Reform*, CTR. FOR DEMOCRACY & TECH. (Dec. 5, 2013), https://www.cdt.org/blogs/mark-stanley/0512day-action-demand-ecpa-reform (seeking reform of the Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848).

15. Fair Credit Reporting Act, 15 U.S.C. § 1681 (2011).

ited to the publication of non-newsworthy facts, the revelation of which would be highly offensive to a reasonable person.[16] The First Amendment compels this limitation, which otherwise would have unacceptable consequences for the freedom of speech.[17] Yet in extreme situations, the tort can and should remain a viable remedy.[18]

In a world of social media, wearable surveillance technologies like Google Glass, facial recognition capabilities and the "Internet of Things," even semi-public and public information (a picture of your face, for example) might be worthy of some protection.[19] Yet precisely because that information is not a secret, the legal protection for it might need to be indirect or weak (i.e., modest) so that the information can be appropriately shared and used in beneficial ways.

A. Porous Coverage

Privacy protections can be said to offer only modest coverage when they do not cover the full range of problematic activities, vulnerable parties, or bad actors in a given context. Some laws only protect certain kinds of information and technologies, such as social media login credentials, and self-disclosed, socially shared information.[20] Critics perceived California's online eraser law as inadequate because it only applied to original instances of uploaded content by the user, not shared or "re-posted" instances of the same information. Other state laws limiting requests for social media access explicitly do not protect information that is in "the public domain," though it is unclear exactly what that term means.[21]

Other limitations in coverage can also be seen as a form of modesty,

16. Neil M. Richards, *The Limits of Tort Privacy*, 9 J. TELECOMM. & HIGH TECH. L. 357, 361 (2011).

17. *See* Florida Star v. B.J.F., 491 U.S. 524 (1989); s*ee also* 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); Neil M. Richards & Daniel J. Solove, *Privacy's Other Path: Recovering the Law of Confidentiality*, 96 GEO. L.J. 123 (2007); Andrew J. McClurg, *Kiss and Tell: Protecting Intimate Relationship Privacy Through Implied Contracts of Confidentiality*, 74 U. CIN. L. REV. 887 (2006).

18. *See, e.g.*, Tecza v. Univ. of S.F., 532 F. App'x 667, 669 (9th Cir. 2013); Vurimindi v. Fuqua Sch. of Bus., 435 F. App'x 129, 135 (3d Cir. 2011); Amato v. Dist. Attorney for Cape & Islands Dist., 952 N.E.2d 400, 410 (Mass. App. Ct. 2011); Yath v. Fairview Clinics, N.P., 767 N.W.2d 34, 42 (Minn. Ct. App. 2009).

19. *See* F.T.C., *supra* note 12; *Internet of Things – Privacy and Security in a Connected World*, FED. TRADE COMM'N, http://www.ftc.gov/news-events/events-calendar/2013/11/internet-things-privacy-and-security-connected-world (last visited Jan. 23, 2014); Gabriel Meister & Benjamin Han, *Peering into the Future: Google Glass and the Law*, SOCIALLY AWARE (Sept. 9, 2013), http://www.sociallyawareblog.com/2013/09/09/peering-into-the-future-google-glass-and-the-law/.

20. *See* CAL. BUS. & PROF. CODE § 22581; *see, e.g.*, MICH. COMP. LAWS ANN. § 37.273; NEV. REV. STAT. § 613.135; N.J. STAT. ANN. § 34:6B-6.

21. *See* 820 ILL. COMP. STAT. ANN. 55/10(b)(3) (2014).

including limited demographic coverage. Some demographics might need privacy protections more than others. This is particularly true for vulnerable populations that are treated differently from the average reasonable person. For example, the Children's Online Privacy Protection Act (COPPA) only protects Internet users under the age of 13.[22] The online eraser law applies to teenagers under 18.[23] Some of the state laws limiting employer access to social media profiles only protect prospective, but not current, employees.[24]

Temporal modesty is a possibility for privacy regulation that has yet to be embraced, but holds great promise as increasingly more aspects of our lives persist in digital form. Not all information needs to be protected eternally. Some information need only be protected during defined periods. This goal has already been recognized with the common law's general reluctance to grant privacy rights to the deceased.[25] What other defined time periods such as residency and employment might be used as benchmarks to limit privacy protections for certain kinds of information like addresses and job searches?

Sunset provisions to force legislative action on certain privacy laws after a set period are possible modest approaches for semi-public information.[26] Sometimes it is difficult to determine when new technologies are genuinely threatening to privacy and when they are simply scary because society is not accustomed to them. This is a complex problem because until society has had a chance to acclimate to a technology, it is impossible to know for sure whether it is problematic.[27] Yet once a technology becomes entrenched, norms surrounding their use are difficult to change.[28]

22. Children's Online Privacy Protection Act, 15 U.S.C. § 6501(1) (2011).

23. CAL. BUS. & PROF. CODE § 22580(d) (effective Jan. 1, 2015).

24. N.M. STAT. ANN. § 50-4-34.

25. *See generally* Lugosi v. Universal Pictures, 603 P.2d 425, 428 (Cal. 1979) (holding that privacy rights created by the invasion of privacy tort do not survive death) (superseded by statute).

26. Emily Berman, *The Paradox of Counterterrorism Sunset Provisions*, 81 FORDHAM L. REV. 1777, 1783 (2013) ("At bottom, sunsets are an institutional design tool that forces Congress to return to policies that, for various reasons, may benefit from review. Based on its reexamination, Congress can then modify the policy, renew it, or allow it to expire."); Rebecca M. Kysar, *Lasting Legislation*, 159 U. PA. L. REV. 1007 (2011).

27. *See, e.g.*, Adam Thierer, Technopanics, *Threat Inflation, and the Danger of an Information Technology Precautionary Principle*, 14 MINN. J.L. SCI. & TECH. 309 (2013).

28. *See, e.g.*, Stephen M. Bainbridge, *Mandatory Disclosure: A Behavioral Analysis*, 68 U. CIN. L. REV. 1023, 1043–44 (2000) ("The so-called "status quo bias" posits a systematic decisionmaking bias pursuant to which actors favor maintaining the status quo rather than switching to some alternative state. The status quo bias can lead to market failure where decisionmakers' preference for the status quo perpetuates suboptimal practices."); Todd Davies, *A Behavioral Perspective on Technology Evolution and Domain Name Regulation*, 21 PAC. MCGEORGE GLOBAL BUS. & DEV. L.J. 1, 4 (2008) ("Other things being equal, most people tend to favor the status quo over a change."); John T. Gourville, *The Curse of Innovation: Why*

When the Facebook feature "News Feed" was unveiled, many feared it would threaten user privacy.[29] In a way, it did. Users were caught off guard by the aggregation of personal information in one place, and felt violated as information they assumed was buried was made prominent to other users.[30] Yet most Facebook users now consider the feature to be one of the most attractive things about the service.[31] The problem was seemingly as much about the rapid and surprising nature of the rollout as it was about the design of the software.

Other useful technologies remain problematic. Useful technologies like GPS, drones, facial recognition, and genetic and biometric identifiers all implicate privacy concerns.[32] Might temporary protections such as sunset provisions and mandatory testing periods be useful here as "speed bumps" of sorts to allow society to properly acclimate to revolutionary technologies? The Federal Aviation Administration is already taking this approach with a gradual embrace of drones, a technology with great promise as well as a capacity for surveillance.[33] During periods of temporary protection, individuals would be able to gradually adjust their behavior, contemplate appropriate norms, and determine which particular aspects or uses of a technology might be problematic and why.

While sunset provisions have an inconsistent track record, there might be some utility in extending a privacy protection for a limited amount of time after some triggering event, such as a disclosure online. For other types of information, it is not immediate disclosure that is problematic, but rather the excavation of information that was long since buried. In that case, perhaps latent privacy protections could be useful after some determined "free use" or "hot" period.[34]

The value of temporary protections is even more apparent when considered along with the dramatic rise in ephemeral online communica-

Innovative New Products Fail (Mktg. Sci. Institute, Working Paper No. 05-117, 2005).

29. Tracy Samantha Schmidt, *Inside the Backlash Against Facebook*, TIME (Sept. 6, 2006), http://content.time.com/time/nation/article/0,8599,1532225,00.html.

30. danah boyd, *Facebook's Privacy Trainwreck*, 14 CONVERGENCE 13 (2008), *available at* http://www.danah.org/papers/FacebookPrivacyTrainwreck.pdf.

31. *See, e.g.*, Roland Irwin, *Opinion: What marketers need to know about Facebook*, ADNEWS (Dec. 20, 2013), http://www.adnews.com.au/news/opinion-what-marketers-need-to-know-about-facebook. ("The news feed has become the primary area of focus and engagement for users.").

32. *See, e.g.*, *Privacy by Topic: The A to Z's of Privacy*, ELEC. PRIVACY INFO. CTR., http://epic.org/privacy/ (last visited Mar. 27, 2014) (providing links to the privacy issues in location data, drones, biometric identifiers, and facial recognition technologies).

33. *See, e.g.*, Ryan Calo, *The FAA's Drone Privacy Plan: Actually Pretty Sensible*, FORBES (Nov. 9, 2013, 6:38 PM), http://www.forbes.com/sites/ryancalo/2013/11/09/the-faas-drone-privacy-plan-actually-pretty-sensible/.

34. The idea of temporal protections has been explored in other areas of the law, such as intellectual property. *See, e.g.*, Victoria Smith Ekstrand, *News Piracy and the Hot News Doctrine: Origins in Law and Implications for the Digital Age*, 15 LAW & SOC'Y REV. 1037, 1037 (2005).

tion. Communication "exploding" services like SnapChat and Frankly highlight the significant role of technologically imposed temporal limitations for privacy.[35] Ephemeral laws and information could play a large role in a regime of modest protection for semi-public information.

B. Indirect or Weak Remedies

Another form of modesty can be measured by how direct, strong, or effective a remedy is. Often remedies do not directly prohibit problematic conduct. Rather, they indirectly obligate or prohibit certain activities as a means to reduce the likelihood of problematic conduct from occurring. For example, laws that restrict an employer from requesting access to a social media profile do not completely prevent that employer from discovering information posted to a profile.[36] That same information might be easily uncovered by co-workers. Damaging information posted to social media might exist elsewhere in publicly accessible records and on the Internet as well. These laws just make it less likely such information will be discovered through social media, a common repository of candid information.

One of the most prevalent modest remedies is mandated disclosure, often known in privacy circles as "notice."[37] Some federal and state laws require that collectors of personal information provide notice to consumers of what information they collect, how they use it, and with whom they plan to share it.[38] At least forty-six states have data breach notification laws, which require companies that have suffered a data breach to inform those possibly affected so that they may respond appropriately.[39]

Mandated disclosure has its critics.[40] It is unlikely that notice will suffice as the sole privacy protection in many contexts. Yet notice can be effective as merely a component of an ongoing privacy regulatory process.[41] This strategy allows policy makers to focus on the modest bene-

35. FRANKLY MESSENGER, http://chatfrankly.com/ (last visited Jan. 23, 2014); SNAPCHAT, http://snapchat.com (last visited Jan. 23, 2014).

36. *See supra* note 5.

37. *See* The Disclosure Crisis [Issue], 88 WASH. L. REV., no. 2 (2013).

38. 45 C.F.R. § 164.520 (2010) (requiring health care providers to provide notice of privacy practices); CAL. BUS. & PROF. CODE § 22581(a) (2013).

39. *See State Security Breach Notification Laws*, NAT'L CONF. STATE LEGIS., http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx (last updated Jan. 21, 2014); *see also* Paul M. Schwartz & Edward J. Janger, *Notification of Data Security Breaches*, 105 MICH. L. REV. 913 (2007).

40. *See, e.g.* Omri Ben-Shahar & Carl E. Schneider, *The Failure of Mandated Disclosure*, 159 U. PA. L. REV. 647, 651 (2011) ("Although mandated disclosure addresses a real problem and rests on a plausible assumption, it chronically fails to accomplish its purpose. Even where it seems to succeed, its costs in money, effort, and time generally swamp its benefits. And mandated disclosure has unintended and undesirable consequences, like driving out better regulation and hurting the people it purports to help.").

41. M. Ryan Calo, *Against Notice Skepticism in Privacy (and Elsewhere)*, 87 NOTRE

fits of notice without committing solely to a privacy protection with significant and acknowledged shortcomings.[42]

Mandated disclosure has the ancillary benefits of compelling companies to audit their privacy practices and create an organizational structure to ensure that even if privacy is not promised, it is not ignored.[43] Those making representations about their data collection and use are also obligated by the Federal Trade Commission (FTC) to be honest.[44] Ryan Calo and others have explored the many different ways beyond unreadable boilerplate text that notice can be given.[45]

Investigation-based remedies can also serve to increase accountability as well as indirectly dissuade privacy invasive activities. For example, the Federal Trade Commission (FTC) and the Consumer Financial Protection Bureau (CFPB) are able to use civil investigative demands and requests for substantiation of efficacy claims in advertising to compel companies to disclose information.[46] The mere possibility of having to turn over information can encourage good behavior, particularly if an investigation can lead to the public disclosure of particular facts or an enforcement action. One of the FTC's central advertising requirements is that of substantiation, which requires that advertisers have a reasonable basis for claims regarding a good or service and be able to produce evidence of such a basis on demand.[47]

DAME L. REV. 1027, 1030 (2012) (arguing against "an extreme skepticism of mandatory notice--a highly popular but much maligned regulatory strategy—by questioning whether critics or proponents of notice have identified and tested all of the available notice strategies").

42. *See, e.g.*, Daniel J. Solove, *Introduction: Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1879, 1886 (2013) ("The evidence suggests that people are not well informed about privacy. Efforts to improve education are certainly laudable, as are attempts to make privacy notices more understandable. But such efforts fail to address a deeper problem--privacy is quite complicated. This fact leads to a tradeoff between providing a meaningful notice and providing a short and simple one.").

43. Peter P. Swire, *The Surprising Virtues of the New Financial Privacy Law*, 86 MINN. L. REV. 1263, 1264-65 (2002) ("[P]ublication of [privacy] notices and the new legal obligation to comply with them have forced financial institutions to engage in considerable self-scrutiny as to their data handling practices. The current notices, even in their imperfect form, have reduced the risk of egregious privacy practices. Improved notices, as described in this Article, would enhance accountability while also communicating far more clearly with ordinary customers.").

44. *See, e.g.*, Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583.

45. *See* Calo, *supra* note 41.

46. *See, e.g.*, 32 Fed. Proc., L. Ed. § 75:58 ("The Federal Trade Commission (FTC) has the power to require by subpoena the attendance and testimony of witnesses and the production of documentary evidence relating to any matter under investigation from any place in the United States at any designated place of hearing."); Joseph T. Lynyak, III & Rebecca Tierney, *Dealing with Civil Investigative Demands from the CFPB: Rules, Responses, and Practice Considerations*, 130 BANKING L.J. 771, 781 (2013).

47. *See, e.g.*, FED. TRADE COMM'N, POLICY STATEMENT REGARDING ADVERTISING SUBSTANTIATION, appended to Thompson Medical Co., 104 F.T.C. 648, 839 (1984), *aff'd*, 791 F.2d 189 (D.C. Cir. 1986), *cert. denied*, 479 U.S. 1086 (1987) ("the Commission has de-

Perhaps the most promising strategy for indirect and modest privacy remedies is to focus on the design of technologies. While data security requirements might seem to companies like direct and robust regulations, they are, in effect, indirect protections against the wrongful access and use of personal information. Given the popularity of "Privacy by Design" and the proper architecture of the Internet of things, it is easy to forget that data security is the most prominent design-based approach to protecting privacy. Virtually every data security professional would likely agree that perfect security is impossible. Data breaches are inevitable.[48] Given the difficulty in directly enforcing laws against hackers and data thieves, the next best alternative would seem to be the implementation of technical and administrative safeguards to reduce the probability of a data breach.[49]

While voluntary and mandatory data security protections are indirect and incomplete in that they do not directly restrain the most culpable actor (the hacker/data thief) and acknowledge the inevitability of certain harms, few would likely categorize the effect of data security laws as "modest." Thus, data security requirements serve as an example of how technically modest indirect protections can be robust in practice by raising the transaction cost to commit a harmful act high enough to dissuade most potential bad actors.[50] This lesson about the effectiveness of probability-based protections can be applied to other proposed and existing laws that are criticized for their modest effect.

For example, a common critique of modern privacy protections is that they are futile because much of what they protect can be discovered

termined that in the future it will rely on nonpublic requests for substantiation directed to individual companies via an informal access letter or, if necessary, a formal civil investigative demand. The Commission believes that tailored, firm-specific requests, whether directed to one firm or to several firms within the same industry, are a more efficient law enforcement technique."); *see also* Charles Shafer, *Developing Rational Standards for an Advertising Substantiation Policy*, 55 U. CIN. L. REV. 1, 4 (1986) ("An advertiser violates the FTCA by making claims about a product when the advertiser does not have a reasonable basis to believe the claim, i.e., the advertiser lacks sufficient substantiation for the claim. This 'reasonable basis doctrine' forms the root of what is known as the Commission's advertising substantiation program. That program involves (or has involved) collecting and disseminating to the public the substantiation for particular advertising claims, as well as penalizing advertisers who make claims without a sufficient substantiation for those claims.").

48. *See, e.g.*, Derek E. Bambauer, *Ghost in the Network*, 162 U. PA. L. REV. 5 (arguing cyberattacks are inevitable and widespread).

49. *See generally* FED. TRADE COMM'N, *supra* note 12 (embracing design based approach to protecting privacy).

50. *See, e.g.*, Woodrow Hartzog & Frederic Stutzman, *The Case for Online Obscurity*, 101 CALIF. L. REV. 1 (2013); Harry Surden, *Structural Rights in Privacy*, 60 SMU L. REV. 1605 (2007) ("Society relies upon…latent structural constraints to reliably inhibit certain unwanted conduct in a way that is functionally comparable to its use of law. For example, society has frequently depended upon the search costs involved in aggregating and analyzing large amounts of information to effectively protect anonymity.").

elsewhere.[51] A similar argument is made by those who believe it is inappropriate to protect "public" information. Yet the term "public information" is just as intractable and difficult to conceptualize as the term "privacy." As it is often used in modern discourse the term "public information" falsely presumes an easy and uniform accessibility in the form of low transaction costs.[52]

Another feature of the online eraser law that has drawn similar criticism is the requirement that companies merely provide a way to "take down" information by making it inaccessible via the Internet, rather than the enablement of a total deletion.[53] In other words, while California teens have the right to remove their own posts from the Internet, they have no right to have the posts completely deleted from the companies' databases. The posts simply become invisible to Internet users, not obliterated. While this feature was criticized for not addressing the harms that are associated with the bulk storage of personal information, the benefits of being able to render posts generally inaccessible should not be marginalized. Many modern privacy threats come not from faceless entities but from those we interact with on a day-to-day basis.[54]

Often, protections for semi-private kinds of information are best understood as raising the transaction costs to obtain, understand, or use certain kinds of information. Elsewhere, I have argued that these kinds of protections protect information that is nominally "public" but practically obscure.[55] Individuals regularly rely upon this obscurity. Criticisms that a law or voluntary protection is ineffective because the information to be protected is already known to others miss the value of obscurity. The modesty of probabilistic protection of semi-private information is precisely the kind of nuanced legal response discussed below that is necessary in an age of hyper socialization.

51. *See, e.g.*, BJ Ard, *Confidentiality and the Problem of Third Parties: Protecting Reader Privacy in the Age of Intermediaries*, 16 YALE J. L. & TECH. 1, 3 (2014); Clark D. Asay, *Consumer Information Privacy and the Problem(s) of Third-Party Disclosures*, 11 NW. J. TECH. & INTELL. PROP. 321 (2013); Helen Nissenbaum, *Protecting Privacy in an Information Age: The Problem of Privacy in Public*, 17 L. & PHIL. 559, 562 (2000), *available at* http://www.nyu.edu/projects/nissenbaum/papers/privacy.pdf.

52. *See* Harry Surden, *supra* note 50.

53. *See* Ferenstein, *supra* note 4.

54. *See, e.g.*, Woodrow Hartzog, *Social Data*, 74 OHIO ST. L. J. 995 (2013).

55. Hartzog & Stutzman, *supra* note 50; Woodrow Hartzog & Frederic Stutzman, *Obscurity by Design*, 88 WASH. L. REV. 385, 397 (2013); *see also* Fred Stutzman & Woodrow Hartzog, *Boundary Regulation in Social Media*, in CSCW'12: PROCEEDINGS OF THE ACM 2012 CONF. ON COMPUTER SUPPORTED COOPERATIVE WORK 769, 773 (2013), *available at* http://dl.acm.org/citation.cfm?id=2145320&dl=ACM&coll=DL&CFID=427864292&CFTOKEN=44076415.

II. WHY SHOULD WE VALUE MODEST PRIVACY PROTECTIONS?

Privacy is a diverse and protean concept, which makes consensus on relevant remedies seem elusive.[56] Perhaps many efficient remedies seem elusive because the parties involved are operating under the belief that a general consensus about the nature of privacy must be reached before the problems related to privacy can be solved. For many different kinds of privacy harms, this belief is mistaken.

In exploring how judges deal with the problems of legal pluralism, Professor Cass Sunstein has proposed that participants in many legal controversies try to produce "incompletely theorized agreements" on particular outcomes as a way to produce agreement among a diverse set of beliefs.[57] In other words, "They agree on the result and on relatively narrow or low-level explanations for it. They need not agree on fundamental principle."[58]

According to Sunstein, "The distinctive feature of this account is that it emphasizes agreement on (relative) particulars rather than on (relative) abstractions. This is an important source of social stability and an important way for diverse people to demonstrate mutual respect, in law especially but also in liberal democracy as a whole."[59] Sunstein gave as an example:

> People may believe that it is important to protect endangered species, while having quite diverse theories of why this is so. Some may stress obligations to species or nature as such; others may point to the role of endangered species in producing ecological stability; still others may point to the possibility that obscure species will provide medicines for human beings. When (and if) people who agree on the same course of action are able to do so from different foundations, they need not choose among foundations.[60]

So it is with privacy. Individuals that differ on first-order questions about the nature and scope of privacy and privacy harm could agree that certain types of information such as financial and health information should be protected without having to come to philosophical agreement about the exact nature of the privacy or the extent of the harm if disclosed. Similarly, modest privacy protections could serve the same function, encouraging people with different ideas to remain in dialogue with

56. *See, e.g.*, Adam Thierer, *The Pursuit of Privacy in A World Where Information Control Is Failing*, 36 HARV. J.L. & PUB. POL'Y 409, 414 (2013).

57. Cass R. Sunstein, *Incompletely Theorized Agreements*, 108 HARV. L. REV. 1733, 1734 (1995) ("Far from having a scale, they must operate in the face of a particular kind of social heterogeneity: sharp and often intractable disagreements on basic principle.").

58. *Id.* at 1735-36.

59. *Id.* at 1736.

60. *Id.*

one another while the larger first-order debates continue as long as they can agree on particular specific remedies.[61] As will be discussed below, modest remedies are generally more acceptable to parties with diverse interests and feasible to compromise. As such, they are ideal objectives for incompletely theorized agreements.

Modest privacy laws can also fill a gap in the protection of personal information. The problem with traditional common law privacy remedies is that they do not scale well. Legal privacy remedies are difficult for most Internet users to utilize.[62] This was less problematic in the pre-digital era. The need to enforce a privacy right was the exception, not the rule.[63] Most personal disclosures were fleeting and few social exchanges were recorded or widely disseminated.[64]

The Internet and other digital technologies have altered the nature and magnitude of personal disclosure. Given the flood of personal information disclosed online, virtually every action taken online can implicate privacy concerns. Yet only a few of these disclosures are considered "private" enough to trigger most traditional privacy remedies.[65] As a result, these exclusive remedies languish or are derided as inappropriate for most kinds of information and relationships.

A better approach to protecting privacy would to openly embrace modest protections in some contexts. It is easy to see why middle ground, modest privacy protections are not as popular or intuitively appealing as either robust protections or the alternative "hands off" approach. Modest protections risk satisfying no one. Those seeking dramatic privacy reforms to counter aggressive surveillance and information collection might seek an omnibus and robust Federal privacy statute.[66] Others feel that even modest privacy protections are an unacceptable cost to commercial information and technology interests. Critics question the imposition of costs to innovation for perceived meager benefits. This polarization of our privacy discourse leaves little room for compromise.

An embrace of modest protections such as design-based strategies, (effective) forms of notice, and indirect prohibitions have several underappreciated benefits. First, modest protections better reflect privacy as

61. I thank Brannon Denning for this insightful point.

62. *See* Richards & Solove, *supra* note 13, at 1889, 1917-19; *see also* DANIEL J. SOLOVE & PAUL M. SCHWARTZ, INFO. PRIVACY LAW 1, 28 (4th ed. 2011).

63. *See* Richards & Solove, *supra* note 13, at 1919-21.

64. *See* Patricia Sanchez Abril, *A (My)space of One's Own: On Privacy and Online Social Networks*, 6 NW. J. TECH. & INTELL. PROP. 73, 75 (2007).

65. Neil M. Richards & Daniel J. Solove, *Prosser's Privacy Law: A Mixed Legacy*, 98 CAL. L. REV. 1887, 1889 (2010) ("Today, the chorus of opinion is that the tort law of privacy has been ineffective, particularly in remedying the burgeoning collection, use, and dissemination of personal information in the Information Age.").

66. Commercial Privacy Bill of Rights Act, S. 799, 112th Cong. (2011).

a heterogeneous concept.[67] There are also many different kinds of privacy harms, not all of which are clear and direct. Modest protections are particularly useful in protecting against harms that are remote, speculative, or cumulative. Second, modest protections are useful in trying to balance privacy protections with other values. Finally, moderate privacy protections are likely more politically palatable than robust ones.

A. Heterogeneous Concepts Like Privacy Need Diverse Protections

One of the most significant problems with traditional privacy law is that it treats information largely in only two ways—public or private.[68] The public/private categorization of information that dominates privacy law has resulted in most civil privacy remedies inapplicable in all but the most dramatic circumstances.[69] A better stratification of privacy remedies could provide for reduced protection for greater amounts of information.

It is tone deaf in the digital age to provide robust protection to a small amount of information and leave the remainder unguarded. Additionally, there is no reason to provide equal protection to all personal information that is deemed "private." Of course, some information, such as passwords and online health records, must remain secret or at least confidential to keep individuals from harm.[70] But less sensitive information, like much of what is disclosed on the social web, can be safely disclosed to many and need only remain obscure.[71]

B. Balance with Competing Values

Privacy protections can conflict with other values such as free speech, transparency, and security. Sometimes this means these values cannot coexist. Yet lower levels of protection for some categories of information based on social norms as well as individual preferences can restore balance for privacy and competing interests.

Professor Paul Ohm has explored how privacy and transparency goals could be balanced by pursuing "good enough privacy," which is achieved by making information "hard but possible" to obtain.[72] Accord-

67. Daniel J. Solove, *Conceptualizing Privacy*, 90 CAL. L. REV. 1087 (2002).

68. *See, e.g.*, Helen Nissenbaum, PRIVACY IN CONTEXT (2010); Daniel Solove, THE DIGITAL PERSONS 42 (2004).

69. *See* Richards, *supra* note 16.

70. *See* 45 C.F.R. § 160 (2013); 45 C.F.R. § 164 (2013).

71. Woodrow Hartzog & Frederic Stutzman, *The Case for Online Obscurity*, 101 CAL. L. REV. 1 (2013).

72. Ohm, *supra* note 5, at 63 ("The problem with balancing two equally important and seemingly unmoving interests is that any time one side prevails on any narrow set of facts, the other side—engaged as it were in a game of brinksmanship—views the result as a loss. This is

ing to Ohm, we can balance the harms of transparency and harm by allowing actors to get the information they want, "but only with hard work."[73] Here, Ohm recognized the value of high transaction costs as a modest protection for personal information.

This dynamic is well illustrated in the debate over transparency in public records that contain personal information. While many citizens do not mind being identified in public records, they feel their privacy has been harmed when those records become easily searchable by any Internet user.[74]

A compromise to honor both privacy and transparency goals could be to post information in disaggregated ways that are not indexed by search engines. Like with Ohm's proposal, those seeking particular records can find them if they are willing to spend the requisite amount of time and effort in locating the records. This would have the effect of reducing harms from idle voyeuristic tendencies as well as scraping and aggregation of the data in bulk in problematic ways that were unintended by the record creator.

For example, consider modest privacy regulations for the burgeoning mugshot industries, which collects mugshot data in bulk from public records repositories and makes them highly visible via search engines.[75] According to New York Times journalist David Segal:

> The ostensible point of these sites is to give the public a quick way to glean the unsavory history of a neighbor, a potential date or anyone else. That sounds civic-minded, until you consider one way most of these sites make money: by charging a fee to remove the image. That fee can be anywhere from $30 to $400, or even higher. Pay up, in other words, and the picture is deleted, at least from the site that was paid. To. . .millions of. . .Americans now captured on one or more of these sites, this sounds like extortion. Mug shots are merely artifacts of an arrest, not proof of a conviction, and many people whose images are now on display were never found guilty, or the charges against them were dropped. But these pictures can cause serious reputational damage.[76]

the "Thunderdome" approach to balancing, a zero-sum endeavor where two opposing principles enter, and only one can emerge victorious.").

73. *Id*. at 49.

74. Michael Hiltzik, *Should CalPERS Post Pensioners' Financial Data Online?*, L.A. TIMES (July 19, 2013), http://articles.latimes.com/2013/jul/19/business/la-fi-hiltzik-20130721.

75. David Segal, *Mugged by a Mug Shot Online*, N.Y. TIMES (Oct. 5, 2013,), http://www.nytimes.com/2013/10/06/business/mugged-by-a-mug-shot-online.html?pagewanted=all&_r=0; David Kravets, *Mug-Shot Industry Will Dig Up Your Past, Charge You To Bury It Again*, WIRED (Aug. 2, 2011, 1:52 PM), http://www.wired.com/threatlevel/2011/08/mugshots/.

76. *Id.*

Hiding information from search engines could also help balance free speech and privacy interests. In previous research, I have argued that instead of the mandatory or voluntary deletion of information from websites altogether, a compromise could be some form of obscurity, where the information is not searchable, hid behind privacy settings, isolated from aggregated data sets, or de-identified.[77] Like the public records scenario described above, speakers would still be allowed to speak and publish information, but information seekers would not be able to find or fully understand the information without some cost.

For example, in the mugshot controversy, according to Segal, the Reporters Committee for Freedom of the Press (RCFP) "favors unfettered access to the images, no matter how obscure the arrestee and no matter the ultimate disposition of the case. Even laws that force sites to delete images of the exonerated, the committee maintains, are a step in the wrong direction."[78] The RCFP views attempts to get the mugshots taken down as an attempt to deny history.[79] Yet there is a clear harm to those who seek to put their past behind them. Making these photos obscure but accessible by removing them from search engines could minimize harm while not completely prohibiting speech.

Regarding the balance of security and privacy, the function of warrants, subpoenas, and any procedural restriction on the government collection of information operates in a way similar to Ohm's suggestion for "pretty good privacy"—they make information hard, but possible to get. The requirement to follow procedure not only ensures a search is justified, but it also imposes a transaction cost that will practically limit the resources spent on surveillance. Ideally, this results in fewer dragnet, suspicionless, and otherwise problematic searches. In a sense, criminal procedural protections were some of the very first protections aimed at decreasing the probability information being found rather than total prevention.

C. Modesty is Palatable

History shows that most proposed privacy protections will not become law.[80] Data security legislation is a perennial favorite, as is some

77. Hartzog & Stutzman, *supra* note 71 at 48.

78. Segal, *supra* note 75.

79. *Id.*

80. *See* Tim Lisko, *112th Privacy Legislation*, PRIVACYWONK, http://www.privacywonk.net/2011/08/112th-privacy-legislation.php (last updated Feb. 7, 2012) (detailing federal legislation proposed in the 112th Congress); Craig Hoffman, *Online Privacy and Data Security Legislation Update – 2011 Year in Review*, DATA PRIVACY MONITOR (Dec. 28, 2011), http://www.dataprivacymonitor.com/federal-legislation/online-privacy-and-data-security-legislation-update-2011-year-in-review/; *EPIC Bill Track Tracking Privacy, Speech, and Cyber-Liberties Bills in the 111th Congress*, EPIC,

form of a privacy bill of rights.[81] There are many reasons these bills are never adopted, but it seems that some lawmakers often balk at the strength of the protection. Privacy protections are usually not without cost, often to business and innovation.

Modest privacy protections can have two important benefits over more broadly worded, all-encompassing protections. First, modest protections are more likely to become law because they can be seen as a compromise. Instead of protecting privacy in one fell swoop, modest protections can cumulatively become robust. In many contexts it might be desirable to decrease the burden on those who collect, use, and share personal information in exchange for the political capital to extend privacy protections to a broader range of information, like semi-private social disclosures and day-to-day activities in public.

Additionally, modest protections can force lawmakers and relevant stake holders to prioritize the harms to be protected against as well as more clearly articulate the goal and justification for a law. The concept of privacy is specific enough to call upon various values that citizens cherish yet it is vague enough to serve as the impetus for a law that covers much more than is justified. By embracing incremental, modest protections, lawmakers can better focus on specific contextual problems, rather than trying to address too many privacy issues in one action.

By temperately responding to various privacy harms, mistakes by legislatures are more tolerable and more easily corrected. Well-intentioned but ill-conceived legislation is more likely to be revisited if it offers modest protection and if the correction is also likely to be modest in nature. In other contexts, self-regulation might be desirable. Here design-based solutions hold great promise. Using design as a benchmark for success would seem to motivate companies to protect privacy rather than the final tally of "harms" allowed. Particularly with respect to social media, design is relatively transparent. In some circumstances it is less costly than expensive civil remedies.

CONCLUSION

Semi-private information like online social disclosures is difficult to protect. Robust privacy protection for this kind of information risks chilling speech that is designed to be shared. Yet individuals often reasonably expect some form of privacy in information shared with some, but not all. How should the law respond?

In his influential article "The Death of Privacy?" Michael Froomkin concluded that, regarding privacy and the law, "[t]here is no magic bul-

http://epic.org/privacy/bill_track.html (last visited Jan. 31, 2014).

81. *E.g.*, Commercial Privacy Bill of Rights Act, S. 799, 112th Cong. (2011).

let, no panacea. If the privacy pessimists are to be proved wrong, the great diversity of new privacy-destroying technologies will have to be met with a legal and social response that is at least as subtle and multi-faceted as the technological challenge."[82] With respect to semi-privacy information, this prediction has borne out in the form of modest privacy protections. Criticism of these relatively weak, indirect, or incomplete protections is often misguided.

It is often worth providing some form of protection to information even if it is shared with other people. These protections do not always need to be vigorous or direct. Design-based solutions, notice, and other indirect protections can be effective when harms are remote and cumulative. In an age of hyper socialization, courts and lawmakers should embrace the modest protection of semi-public information and recognize that the wide diversity of privacy harms require equally diverse solutions.

82. A. Michael Froomkin, *The Death of Privacy?*, 52 STAN. L. REV. 1461, 1543 (2000).