Brooklyn Law Review

Volume 84 | Issue 2 Article 5

1-1-2019

Pay For (Privacy) Performance: Holding Social Network Executives Accountable for Breaches in Data Privacy Protection

Lital Helman

Pay for (Privacy) Performance

HOLDING SOCIAL NETWORK EXECUTIVES ACCOUNTABLE FOR BREACHES IN DATA PRIVACY PROTECTION

Lital Helman†

INTRODUCTION

Over the past decade and a half, social networking online has grown exponentially, attracting a multitude of users and drawing an increasing volume of online activity.[1] Throughout

† Senior Lecturer of Law, Ono Academic College, Israel. The author would like to thank Sharon Hannes for insights regarding the field of executive compensation and for help in harnessing this field to tackle contemporary privacy challenges. The author also thanks Gideon Parchomovsky, Joel Reidenberg, James Grimmelman, Colleen Chien, Eric Goldman, Helen Nissenbaum, Michael Birnhak, Malte Zieovitz, Miriam Bitton, Sasha Romanovsky, Heather West, Anneleis Mores, Jos Floor, Stephen Deadman, and Guy Pessach, as well as the participants of the New York University Intellectual Property Faculty Workshop, the New York University Privacy Research Group workshop, the 2015 Amsterdam Privacy Conference, the Data Transparency Lab at the MIT Media Lab, and the 2017 Santa Clara University Works In Progress Workshop for helpful comments.

[1] Facebook, the largest social network in the world, alone reported 1.4 billion active daily users in the fourth quarterly report of 2017. Press Release, Facebook, Facebook Reports Fourth Quarter and Full Year 2017 Results (Jan. 31, 2018), https://investor.fb.com/investor-news/press-release-details/2018/Facebook-Reports-Fourth-Quarter-and-Full-Year-2017-Results/default.aspx [https://perma.cc/6Y29-KRGQ]; *see also* danah boyd, *Social Media: A Phenomenon to Be Analyzed*, SOC. MEDIA + SOC'Y, Apr.– June 2015, at 1, 2 ("Over the last decade, social media has gone from being a dream of Silicon Valley technologists to a central part of contemporary digital life around the world."); MAEVE DUGGAN ET AL., PEW RES. CTR., SOCIAL MEDIA UPDATE 2014, at 2 (2015), http://www.pewinternet.org/files/2015/01/PI_SocialMediaUpdate20144.pdf [https://perma.cc/7VGT-H79B] (noting that most Americans use more than one social media platform, and use it increasingly more often); Fred Stutzman, Ralph Gross & Alessandro Acquisti, *Silent Listeners: The Evolution of Privacy and Disclosure on Facebook*, 4 J. PRIVACY & CONFIDENTIALITY, no. 2, 2012, at 7, 7, https://journalprivacyconfidentiality.org/index.php/jpc/article/view/620/603 [https://perma.cc/YD6P-9R24] ("Virtually all US teenagers use social network sites, as well as almost half of all US online adults—an approximate five-fold increase since 2005."); *How to Win Friends and Influence People*, ECONOMIST (Apr. 9, 2016) https://www.economist.com/briefing/2016/04/09/how-to-win-friends-and-influence-people [https://perma.cc/8DRQ-4KGY] (noting that "22% of the internet time Americans spend on mobile devices" is spent on Facebook).

this growth process, social networks have amassed vast quantities of data on individuals all over the world.[2]

Social networks are platforms that allow users to interact with each other online. The business models of social networks involve using users' data in transactions with paying third parties.[3] Indeed, users of social network services typically pay insignificant or no fees for their use of the services.[4] Rather, they provide data about themselves, which the service monetizes via agreements with third parties.[5] These agreements primarily involve blending personalized ads in users' interfaces over the platform, based on a rigorous analysis of users' personal data conducted by the social network.[6]

Designing standards for use of personal data on social media is a fundamental task. On the one hand, experimentation with the new business model can enhance the use of social networking and the value all parties receive in these interactions.[7] On the other hand, the potential harms to privacy this data-sharing business model entails may yield a substantial welfare loss, and in the long term create a chilling effect on desired uses of social media.[8]

---

[2] *See* Stacy-Ann Elvy, *Paying for Privacy and the Personal Data Economy*, 117 COLUM. L. REV. 1369, 1384–87 (2017) (discussing the "data-as-payment model" of social media and other types of firms).

[3] *See* danah m. boyd & Nicole B. Ellison, *Social Network Sites: Definition, History, and Scholarship*, 13 J. COMPUTER-MEDIATED COMM. 210, 211 (2008), https://onlinelibrary.wiley.com/doi/full/10.1111/j.1083-6101.2007.00393.x [https://perma.cc/U6NW-7R3G] (defining the user-facing function of social networks as "web-based services that allow individuals to (1) construct a public or semi-public profile within a bounded system, (2) articulate a list of other users with whom they share a connection, and (3) view and traverse their list of connections and those made by others within the system.").

[4] Elvy, *supra* note 2, at 1385 ("[C]onsumers generally provide their data (and perhaps their attention) to companies when using products that are described as 'free.'").

[5] *See* Chris Jay Hoofnagle & Jan Whittington, *Free: Accounting for the Costs of the Internet's Most Popular Price*, 61 UCLA L. REV. 606, 628 (2014) (discussing Facebook's business model); Howard A. Shelanski, *Information, Innovation, and Competition Policy for the Internet*, 161 U. PA. L. REV. 1663, 1678 (2013) (describing user data as a "[c]ritical [a]sset"); Somini Sengupta, *Facebook Posts Largest Single Day Gain*, N.Y. TIMES: BITS (Oct. 24, 2012, 5:03 PM), http://bits.blogs.nytimes.com/2012/10/24/facebook-posts-largest-single-day-gain-after-third-quarter-earnings-call [https://perma.cc/9QV8-DDXL] (noting that Facebook's revenues stem mostly from "offering marketers a chance to target tailored advertisements . . . on what [users] reveal about themselves").

[6] *See generally* HOWARD BEALES, NETWORK ADVERT. INITIATIVE, THE VALUE OF BEHAVIORAL TARGETING 6–11 (2010), http://www.networkadvertising.org/pdfs/Beales_NAI_Study.pdf [https://perma.cc/S7K2-HNNJ] (discussing behavioral advertising); David S. Evans, *The Online Advertising Industry: Economics, Evolution, and Privacy*, 23 J. ECON. PERSP. Summer 2009, at 37, 42 (2009); Avi Goldfarb & Catherine Tucker, *Online Advertising*, 81 ADVANCES IN COMPUTERS 289, 292–94 (2011); Catherine E. Tucker, *The Economics of Advertising and Privacy*, 30 INT'L. J. INDUS. ORG. 326, 326 (2012).

[7] *See, e.g.*, boyd & Ellison, *supra* note 3 at 214–19.

[8] *See infra* note 108 and accompanying text.

The United States has primarily employed market solutions to tackle the challenge of social media privacy. Under this framework, each social network firm designs its own privacy standards, and users can select whether to use the service based, *inter alia*, on these standards.[9] The Federal Trade Commission (FTC) supervises this process under its authorization to regulate unfair or deceptive acts or practices in or affecting commerce.[10]

As analyzed below, this approach has created a powerful incentive for social network firms to undersupply privacy protection. The reason for the creation of such an incentive is that users are ill-positioned to bargain for better privacy terms on social media, and their privacy interests are eclipsed by a powerful competitive pressure to maximize the collection, analysis, and sale of users' personal data.[11]

Current executive compensation models exacerbate this problem. The standard executive compensation package is a Pay for Performance scheme, where compensation is tied to a firm's economic performance.[12] Such compensation packages motivate executives of social media companies to externalize the costs associated with overexploitation of users' data. These compensation packages also encourage executives to take excessive risks and pursue short- to medium-term profits—even at the expense of the long-term interest of shareholders to maintain users' trust in the system.[13]

In this article, I propose a promising way to reverse the incentives of social media executives to alleviate privacy abuses on social networks—to link the executive compensation in social network firms to the firm's data protection practices. Concretely, I propose to augment the classical incentive contract—in which officers receive a fixed wage and a payment that is tied to the price of the firm's stock—by a payment that depends on a privacy rating. The rating would be determined annually by measuring users' awareness and satisfaction of the privacy practices that their social networks deploy. Privacy officers at firms would be responsible for

---

[9] *See infra* notes 21–25 and accompanying text.

[10] *See* Federal Trade Commission Act, ch. 311, § 5, 38 Stat. 717, 719 (1914) (codified as amended at 15 U.S.C. § 45(a) (2012)) (commonly referred to as the FTC's Section 5 jurisdiction).

[11] *See infra* Section II.A.

[12] *See generally* LUCIAN BEBCHUK & JESSE FRIED, PAY WITHOUT PERFORMANCE: THE UNFULFILLED PROMISE OF EXECUTIVE COMPENSATION 6 (2004) ("[I]n the beginning of the 1990s, prominent financial economists such as Michael Jensen and Kevin Murphy urged shareholders to be more accepting of large pay packages that would provide high-powered incentives."). For the rationale of tying agents' economic interests to their principals' objectives in general, *see* Joseph E. Stiglitz, *Incentives, Risk, and Information: Notes Towards a Theory of Hierarchy*, 6 BELL J. ECON. 552, 570 (1975).

[13] *See infra* Section II.A.

applying the model in the firm, and the compensation committee of the firm would be tasked with incorporating this score into the compensation of key executives.[14]

My proposal is different from existing proposals to fix privacy inefficiencies in two significant ways. First, the policy is not directly aimed at social networking firms. Rather, it is set to influence executives within the firms by manipulating their pay to reflect the benefits and harms that their conduct inflicts. Second, this proposal offers a dynamic solution, where the level of privacy protection on social networks would adapt to the changing privacy standards of society, rather than a static policy where privacy standards are set top-down, via legislation or regulation, and remain constant.[15]

This proposal would dramatically improve privacy protection on social media. It would compel executives to embrace privacy considerations in their decision-making process ex ante and would curb their incentives to surrender users' privacy in pursuit of short-term profits. As a result, it would both enhance the privacy protection users enjoy, and align the interests of executives with the long-term interests of the firm to maintain users' trust in social networks.

Clearly, numerous other businesses besides social networks collect users' data, including retail businesses, network providers, search engines, webhosts, and others. Yet social networks comprise the only platform whose business model revolves exclusively around enticing sharing, analyzing the shared information, and exploiting it to the fullest with third parties.[16] In light of this business model, it is not surprising that the scope of personal information revealed on social networking

---

[14] *See infra* Section II.B. The Compensation Committee is a sub-committee of the Board, composed of three or four independent directors. *See* BEBCHUK & FRIED, *supra* note 12, at 24; *see also* NASD Rule 4350(c)(3); NYSE, Listed Co. Manual Rule § 303A.05, http://wallstreet.cch.com/LCMTools/PlatformViewer.asp?selectednode=chp%5F1%5F4%5F3&manual=%2Flcm%2Fsections%2Flcm%2Dsections%2F [https://perma.cc/7AVT-WKY2]; American Stock Exchange Company Guide §§ 121, 801–809 (2008); Order Approving NYSE and NASDAQ Proposed Rule Changes Relating to Corporate Governance, Exchange Act Release No. 34-48745, 68 Fed. Reg. 64,154 (Nov. 4, 2003); Order Approving AMEX Proposed Rule Changes Relating to Corporate Governance, Exchange Act Release No. 34-48863, 68 Fed. Reg. 68,432, (Dec. 1, 2003).

[15] *See generally* ARTICLE 29 DATA PROTECTION WORKING PARTY, GUIDELINES ON THE IMPLEMENTATION OF THE COURT OF JUSTICE OF THE EUROPEAN UNION JUDGMENT ON "GOOGLE SPAIN AND INC V. AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (AEPD) AND MARIO COSTEJA GONZÁLEZ" C-131/12 (2014) https://www.pdpjournals.com/docs/88502.pdf [https://perma.cc/K3DQ-QM5Y] (providing guidelines on implementing the Right to be Forgotten in the Court of Justice of the European Union).

[16] *See, e.g.*, Nathan Newman, *The Costs of Lost Privacy: Consumer Harm and Rising Economic Inequality in the Age of Google*, 40 WM. MITCHELL L. REV. 849, 865 (2014) (discussing Facebook's and Google's business model).

sites is substantially greater, in both quality and quantity, than on other platforms.[17] It is also not surprising that anonymous use or registration under fake identities are forbidden, and that information is even collected involuntarily, generating privacy externalities and distributive implications.[18] Unlike most other businesses, the market of social networks also tends to consolidate, which curbs the creation of a privacy market.[19] As a result, while privacy risks occur on various types of platforms, they are dramatically exacerbated in the social networking realm.

This article unfolds as follows. Part I explains the current data protection law in the United States and its shortcomings in the context of social media. In this framework, I discuss the limits of consent mechanisms, and show that firms' incentives to internalize privacy concerns are curbed by substantial market failures. I also demonstrate that data use has externalities on other users and non-users of social media, which means that privacy costs can be inflicted upon individuals regardless of their conscious choice. Part II delineates the proposal and explains its advantages. This Part explains the rationale to manipulate executive compensation in the context of privacy protection, and define the steps needed in order for the model to achieve the expected advantages. Part III tackles potential objections to this model. In this framework, I address potential manipulations of the model, as well as the claim that privacy violations are "victimless crimes." This Part also explains the rationale to harness executive compensation to improve privacy interests, rather than to promote other societal values, and explores potential extensions of this idea. A short conclusion ensues.

I. THE LEGAL FRAMEWORK IN THE UNITED STATES

The challenge of protecting privacy online preoccupies lawmakers all over the world.[20] The United States has, with few

---

[17] *See infra* note 54 and accompanying text.

[18] *See infra* notes 90–93 and accompanying text.

[19] *See infra* notes 99–101 and accompanying text.

[20] Various jurisdictions adopted a combination of legal, regulatory, and organizational solutions. *See, e.g.*, Graham Greenleaf, *Global Data Privacy Laws 2017: 120 National Data Privacy Laws, Including Indonesia and Turkey*, 145 PRIVACY LAWS & BUS. INT'L REP. 10–13 (UNSW Law Research, Working Paper No. 17-45), https://ssrn.com/abstract=2993035 [https://perma.cc/9TF2-E88G] ("In the past two years, the number of countries that have enacted data privacy laws has risen from 109 to 120, a 10% increase, with at least 30 more countries having official Bills for such laws in various stages of progress."); *see also* Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) 2016 O.J. (L 119) 1–88. Notably, the EU data protection laws have traditionally had a considerable global effect.

exceptions, fostered self-regulation and market solutions.[21] Accordingly, in most cases in the United States, individual firms, and in some contexts, industry groups, determine their own level of privacy protection.[22]

The FTC oversees this self-regulation regime, relying on its broad powers under Section 5 of the FTC Act "to prevent . . . unfair or deceptive acts or practices in or affecting commerce."[23] Based on this authorization, the FTC requires firms to provide users with notice that details the firm's data management policies, and to follow the policies they set forth. Acting in this capacity, the FTC has also investigated companies—including social networks—regarding their use of user data.[24] The FTC is in fact in the midst of such an investigation with regards to the Cambridge Analytica scandal, where Facebook compromised the data of fifty million users.[25]

The FTC requirements of notice and consent were translated in the market into adopting "Privacy Policies"—documents that describe the firm's practices of collection and use of personal data—and placing these documents on the firm's website.[26]

See generally Michael D. Birnhack, *The EU Data Protection Directive: An Engine of a Global Regime*, 24 COMPUTER L. & SECURITY REP. 508 (2008) (examining the emerging global legal regime that attempts to regulate various aspects of personal data); *see also* Kenneth A. Bamberger & Deirdre K. Mulligan, *Privacy on the Books and on the Ground*, 63 STAN. L. REV. 247, 261 (2011) (noting that large firms have added a new C-level position of Chief Privacy Officer to reflect internally on the firm's privacy conduct).

[21] *See* Bamberger & Mulligan, *Privacy on the Books*, *supra* note 20, at 251 ("Congress has declined to follow the European model of a dedicated privacy administrator."); Marc Rotenberg, *Fair Information Practices and the Architecture of Privacy (What Larry Doesn't Get)*, 2001 STAN. TECH. L. REV. 1, 2 (2001) (describing the debate between self-regulation and market solutions, and privacy rights and regulation); Dennys Marcelo Antonialli, Note, *Watch Your Virtual Steps: An Empirical Study of the Use of Online Tracking Technologies in Different Regulatory Regimes*, 8 STAN. J. C.R. & C. L. 323, 333 (2012) ("In the United States, the debate revolves around improving the self-regulatory regime, rather than adopting a more normative framework.").

[22] Since no federal law requires privacy protection measures, the FTC can only enforce privacy rules indirectly, via false representation. *See* Federal Trade Commission Act, ch. 311, 38 Stat. 717, 717–24 (1914) (codified as amended at 15 U.S.C. §§ 41–58 (2012)). Examples for industry group regulation include, *inter alia*, the "Digital Advertising Alliance (DAA) Self-Regulatory Program" for online behavioral advertising, which enables users to opt out of some targeted advertising, and "www.aboutads.info," a partnership of public and private parties, which provides information about online advertising. *See* DIGITAL ADVERTISING ALLIANCE (DAA) SELF-REGULATORY PROGRAM, http://www.aboutads.info/ [https://perma.cc/S6NG-ZTGG].

[23] Federal Trade Commission Act, ch. 49, sec. 3, § 5(a), 52 Stat. 111, 111–12 (1938) (codified as amended at 15 U.S.C. § 45 (2012)) (often referred to as Section 5 jurisdiction).

[24] For example, in recent years, both Facebook and Google settled FTC complaints for violating their own policies. *See In re* Facebook Inc., No. C-4365, 2012 WL 3518628, *3 (F.T.C. July 27, 2012); *In re* Google Inc., No. C-4336, 2011 WL 5089551, *7 (F.T.C. Oct. 13, 2011).

[25] Louise Matsakis, *The FTC Is Officially Investigating Facebook's Data Practices*, WIRED (Mar. 26, 2018, 12:05 PM), https://www.wired.com/story/ftc-facebook-data-privacy-investigation/ [https://perma.cc/ELR2-DURR].

[26] *See* Antonialli, *supra* note 21, at 341 (finding that websites typically comply with the FTC's notice requirement by adopting a Privacy Policy). Prominent networks require

This market-based regime has exceptions for certain areas that are subject to stricter federal rules, such as medical or financial information[27] and information of children under thirteen years old.[28] Some state laws have also taken a more interventionist approach across the board, with some spillover effects on other states.[29] Social networks, however, generally fall outside the regulated categories, and are thus free to design their own privacy practices, as long as they publicize their standards and comply with them.[30]

The theory behind market solutions in the social networking realm may sound rather compelling. Social networks form two-sided platforms that connect users on the one hand and advertisers on the other.[31] *See Figure 1.* The best interest of social networks, the theory goes, is to remain competitive on both sides

---

mobile apps to adopt privacy policies as well. *See* Joint Statement of Principles, Office of Att'y Gen. Kamala D. Harris (Feb. 22, 2012), http://ag.ca.gov/cms_attachments/press/pdfs/n2630_signed_agreement.pdf [https://perma.cc/VY63-QKAM] (joined by California Attorney General Kamala D. Harris, Amazon, Inc., Apple, Inc., Google, Inc., Hewlett-Packard Co., Microsoft Corp., and Research in Motion, Ltd.).

[27] *See* Privacy Act of 1974, Pub. L. No. 93-579, 88 Stat. 1896 (codified as amended at 5 U.S.C. § 552a (2012)); Federal Information Security Management Act of 2002, Pub. L. No. 107-347, 116 Stat. 2946, 2946–61 (codified as amended at 44 U.S.C. §§ 3541–3549 (2012)). This "patchwork" approach to privacy regulation has attracted critique even very early on. *See, e.g.*, Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1632 (1999).

[28] *See* Children's Online Privacy Protection Act of 1998, Pub. L. No. 105-277, 112 Stat. 2681–728 ("COPPA") (codified as amended at 15 U.S.C. §§ 6501–6506 (2012)). Other areas where privacy standards are predefined include, for example, limitations on the collection of personal data by government agencies, and limits on the interception of electronic data transmissions in the context of employment. Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended at scattered sections of 18 U.S.C. (2012)).

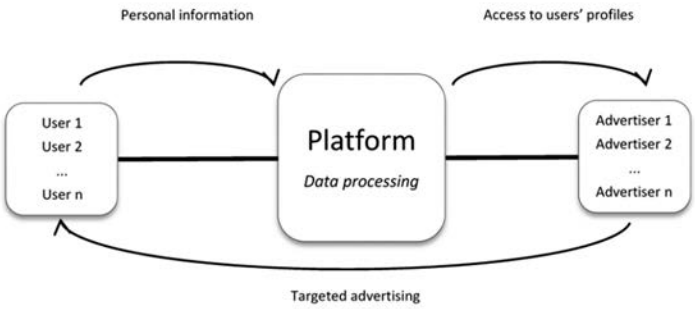
[29] California emerges as a leader in the privacy area, focusing mainly on limitations on data trading (rather than data collection). Part of the Californian law has become the de-facto national standard. *See, e.g.*, California Online Privacy Protection Act, CAL. BUS. & PROF. CODE §§ 22575–22579 (West 2018) (imposing certain requirements on privacy policies regarding California resident consumers). Further, driven by the continued rise of consumer data breaches, California passed the California Consumer Privacy Act (CCPA) in 2018. California Consumer Privacy Act of 2018 ("CCPA"), CAL. CIV. CODE §§ 1798. While the CCPA is likely to undergo substantial changes, it clearly sets to strengthen privacy protection in California, with likely spillover to the United States as a whole.

[30] To avail themselves of limitative legislation, social networks typically ban minors from the service. Many privacy policies also refer to "California resident rights." *See supra* note 28.

[31] *See* Claus-Georg Nolte, Christian Zimmermann, & Günter Müller, No Privacy in Monopoly?: An Economic Perspective on Social Network Services and Data-Centric Business 1 (Oct. 2015) (unpublished manuscript) (on file with author); Shelanski, *supra* note 5, 1677–78 (discussing "the multisided nature of digital platforms"). *See generally* David S. Evans, *The Antitrust Economics of Multi-Sided Platform Markets*, 20 YALE J. ON REG. 325 (2003) (applying the analysis of two-sided platforms to online platforms); Katherine J. Strandburg, *Free Fall: The Online Market's Consumer Preference Disconnect*, 2013 U. CHI. LEGAL F. 95 (2013).

of the market, namely, users and advertisers.[32] Excessive privacy intrusions by social networks would supposedly reduce the demand for the service on the users' side, by an amount exactly related to how much users value their privacy.[33] Following sinking popularity among users, the platform's appeal to advertisers would plummet as well.[34] This projected effect should provide an incentive for firms to internalize users' privacy concerns ex ante.[35] The process of weighing users' concerns against advertisers' willingness to pay for personal data should in theory yield an optimal level of privacy protection.[36]

Figure 1



[32] *See* Jean-Charles Rochet & Jean Tirole, *Two-sided Markets: A Progress Report*, 37 RAND J. ECON. 645, 646 (2006) ("A platform's usage or variable charges impact the two sides' willingness to trade once on the platform and, thereby, their net surpluses from potential interactions; the platforms' membership or fixed charges in turn condition the end-users' presence on the platform.").

[33] *See* Shelanski, *supra* note 5, at 1688–89 (noting that "holding price, service quality, and everything else constant, digital platform customers would rather reveal less information about themselves, and would prefer that those platforms maintain strong, rather than weak, privacy policies regarding the data that customers do disclose"); *see also* Joseph Farrell, *Can Privacy Be Just Another Good?*, 10 J. TELECOMM. & HIGH TECH. L. 251, 254–55 (2012) (modeling users' demand as related to shifts in privacy policies).

[34] As Richard Epstein explains, "in a two-sided market, the ability to attract customers on one side of the market depends on the ability to attract those customers to the other side of the market." *See* Richard A. Epstein, *The Constitutional Paradox of the Durbin Amendment: How Monopolies Are Offered Constitutional Protections Denied to Competitive Firms*, 63 FLA. L. REV. 1307, 1323 (2011).

[35] Michael Birnhack & Niva Elkin-Koren, *Does Law Matter Online?: Empirical Evidence on Privacy Law Compliance*, 17 MICH. TELECOMM. & TECH. L. REV. 337, 339–40 (2011) (showing that when there is user outrage, firms respond to market demands, or at least represent that they do).

[36] *See generally* THOMAS M. LENERD & PAUL H. RUBIN, PRIVACY AND THE COMMERCIAL USE OF PERSONAL INFORMATION: THE CASE OF CUSTOMER PROPRIETARY NETWORK INFORMATION (2007) (finding a functioning market for privacy); Richard A. Posner, *An Economic Theory of Privacy*, 2 REG. 19, 26 (1978); Richard A. Posner, *Privacy, Secrecy, and Reputation*, 28 BUFF. L. REV. 1 (1979); Richard A. Posner, *The Economics of Privacy*, 71 AM. ECON. REV. 405 (1981); Richard A. Posner, *The Right of Privacy*, 12 GA. L. REV. 393, 393 (1978) (comparing theories of privacy).

Reality, however, does not bear out this theory.[37] Under the current regime, it is rational for social networking firms to undersupply privacy protection. As the theory predicts, social networks have a powerful incentive to exploit to the fullest personal information they retain on individuals in order to sell advertisers a palatable product: targeting audiences with great precision.[38] The balance that the theory predicts, however, rarely occurs: as I discuss herein, market failures make users ill-positioned to bargain for privacy ex ante or to act upon privacy harms ex post.[39] Social media users are subject to information problems and face persistent issues with assessing privacy risks and making decisions that affect their privacy. Users also have very little choice, considering the lack of meaningful alternatives, coupled with the powerful societal expectation to maintain an online presence. On top of all that, users face lock-in effects, which makes backing out of social media use nearly impossible.[40] Social network firms rationally respond by favoring advertisers' interests for vigorous exploitation of users' data over a more robust privacy protection.[41]

A predominant market failure that prevents users from bargaining for better privacy terms concerns information problems.[42] While the adoption of privacy policies is widespread,

---

[37] *See, e.g.*, Jack Hirshleifer, *Privacy: Its Origin, Function, and Future*, 9 J. LEGAL STUD. 649, 663–64 (1980); H. Brian Holland, *Privacy Paradox 2.0*, 19 WIDENER L.J. 893, 900–02 (2010) (doubting the functioning privacy market); Richard S. Murphy, *Property Rights in Personal Information: An Economic Defense of Privacy*, 84 GEO. L.J. 2381, 2402 (1996) ("[T]he typical transaction between a merchant or seller and a consumer increasingly can be characterized as an exchange of goods or services for money *and information*."); George J. Stigler, *An Introduction to Privacy in Economics and Politics*, 9 J. LEGAL STUD. 623, 627 (1980) ("[I]n voluntary transactions there is no reason to interfere to protect one party provided the usual conditions of competition prevail; the efficient amount of information will be provided in transactions, given the tastes of the parties for knowledge and privacy.")

[38] Steven Hodson, *The Great Privacy Con of Social Media and Web 2.0*, INQUISITR (Mar. 16, 2010), http://www.inquisitr.com/66776/the-great-privacy-con-of-social-media-and-web-2-0/#rcgSyKVBecZ6ZeIZ.99 [https://perma.cc/CZT3-NTJV] ("It is that constant flow of data that is collected, correlated, mashed up with data from other sources and then put through a strainer for advertisers and marketers to feast upon—for a pretty penny at that."); *see also* James Grimmelmann, *Saving Facebook*, 94 IOWA L. REV. 1137, 1150–51 (2009).

[39] *See* Allen P. Grunes, *Another Look at Privacy*, 20 GEO. MASON L. REV. 1107, 1112 (2013) ("Firms do compete on privacy protection . . . . But this dimension of competition is not very widespread or intense today.").

[40] To address this concern, the General Data Protection Regulation (GDPR)—the most recent European regulation intended to strengthen and unify data protection within the European Union—has a portability rule. *See* Regulation (EU) 2016/679, art. 20, 2016 O.J. (L 119) 1–45.

[41] *See* Schwartz, *supra* note 27, at 1682–83 (discussing the "one-sided bargains that benefit data processors").

[42] ROBERT COOTER & THOMAS ULEN, LAW AND ECONOMICS 41 (2d ed. 1997) (discussing information asymmetries as a standard cause of market failure); Hal R.

privacy policies are notoriously vague, uninformative and noncommittal, they change frequently, and often require ex ante consent to future unspecified changes in the policy.[43] Privacy settings are also complex and fine-grained, and are thus difficult to understand and virtually impossible to use as a basis for comparison between social networks.[44]

The uninformative nature of privacy policies need not come as a surprise. Policies that detail actual data-management practices could only harm firms' interests. Such policies may scare users away and limit uses of personal data if the business model changes in the future, or if the firm merges into another firm with a different agenda on data use.[45] Informative privacy policies would also allow the FTC to spot deviations from the policy and would thus ironically invite more scrutiny. As a result, firms have a powerful incentive to keep privacy policies, in James Grimmelmann's words, "beautiful[ly] irrelevan[t]."[46]

Varian, *Economic Aspects of Personal Privacy*, in INTERNET POLICY AND ECONOMICS 101, 104 (William H. Lehr & Lorenzo Maria Pupillo eds., 2d ed. 2009) ("several of the problems with personal privacy arise because of the *lack* of information available between concerned parties."); Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193, 1253 (1998) ("[I]ndividuals today are largely clueless about how personal information is processed through cyberspace.").

[43] *See, e.g.*, Michael J. Kasdan, *Is Facebook Killing Privacy Softly?: The Impact of Facebook's Default Privacy Settings on Online Privacy*, 2 N.Y.U. INTELL. PROP. & ENT. L. LEDGER 107, 111 (2011) (discussing the 2009 change in Facebook Privacy Policy); Lior Jacob Strahilevitz & Matthew B. Kugler, *Is Privacy Policy Language Irrelevant to Consumers?*, 45 J. LEGAL STUD. S69, S92–93 (2016) (discussing the implications of the "vague and imprecise" nature of privacy policies); James Temperton, *AVG Can Sell Your Browsing and Search History to Advertisers*, WIRED (Sept. 18, 2015), http://www.wired.co.uk/news/archive/2015-09/17/avg-privacy-policy-browser-search-data [https://perma.cc/2G5X-PSHZ] (discussing AVG's 2015 update of its privacy policy to allow sale of users' data); *see also How to Win Friends and Influence People*, *supra* note 1 ("Facebook has a history of hastily changing its privacy policy and the information it shares in public.").

[44] *See* Janice Y. Tsai et al., *The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study*, 22 INFO. SYS. RES. 254, 254 (2011) ("70% of people surveyed disagreed with the statement 'privacy policies are easy to understand', and few people make the effort to read them." (internal citations omitted)); *see also* Antonialli, *supra* note 21, at 343 ("[C]ompanies [have] the ability to notify users only about what they choose to and not about what they ought to.").

[45] *See* Paul Ohm, *Branding Privacy*, 97 MINN. L. REV. 907, 916 (2013) (discussing pivots firms take after amassing large databases of users' personal data). Firms might also be merged into another firm with a different data use agenda. *See, e.g.*, Parmy Olson, *Facebook Is Committed to WhatsApp Encryption, but Could Bypass It Too*, FORBES (Sept. 27, 2018, 3:54 PM), https://www.forbes.com/sites/parmyolson/2018/09/27/facebook-is-committed-to-whatsapp-encryption-but-could-bypass-it-too/#4e17488f3efe [https://perma.cc/PT2S-7K5A] (quoting Facebook's spokesperson following WhatsApp's acquisition that "there are no plan[s] to change" the encryption feature of WhatsApp, but noting also that Facebook has ways to bypass this feature).

[46] *See* Grimmelmann, *supra* note 38, at 1181.

The irrelevance of privacy policies produces an adverse dynamic effect as well.[47] Users rationally respond to the uninformative nature of privacy policies by not wasting time on reading them in the first place.[48] As a result, firms learn that they cannot benefit from adopting robust privacy policies, and draft them ever more vaguely, in turn feeding the disincentive of users to read privacy policies.[49]

Other than these vague privacy policies, users have no other way to learn about data management practices of social networks.[50] They have no way to know what information about them has been collected, how it has been analyzed and used, and who has access to it.[51] Data collection, analytics, and sales occur behind the scenes, and much of that activity is protected as trade secrets.[52] Nor do users know what other information firms (or

---

[47] As Paul Ohm explains, "Ultimately, exposing users to an ever-shifting landscape of broken promises of privacy, in which every privacy policy is inconstant, whittles away expectations of privacy." Ohm, *supra* note 45, at 926.

[48] Aleecia M. McDonald & Lorrie F. Cranor, *The Cost of Reading Privacy Policies*, 4 I/S J.L. & POL. 540, 565 (2008) ("[I]f Americas were to read online privacy policies word-for-word, we estimate the value of time lost as about $781 billion annually.").

[49] *See* Shelanski, *supra* note 5 at 1690 ("If consumers cannot tell whether a firm uses and protects data well or poorly, platforms will lack incentive to choose comparatively pro-consumer policies."). Counterintuitively, there is some evidence that users "punish" firms that proactively bring privacy to the front of the conscious, even if to enhance privacy protection or control over data. Apparently, reference to privacy concerns raises dormant concerns. *See* Leslie K. John, Alessandro Acquisti, & George Loewenstein, The Best of Strangers: Context Dependent Willingness to Divulge Personal Information, 9–10 (July 6, 2009) (unpublished manuscript) http://ssrn.com/abstract=1430482 [https://perma.cc/783Y-QEXV] ("In situations in which privacy concerns are activated, . . . it is likely that people will fail to divulge information even when the risks of doing so are low . . . .").

[50] *See* Kenneth A. Bamberger & Deirdre K. Mulligan, *New Governance, Chief Privacy Officers, and the Corporate Management of Information Privacy in the United States: An Initial Inquiry*, 33 LAW & POL'Y 477, 499 (2011) (citing an interview with an executive: "I hate to say 'what they don't know won't hurt them,' but that's really how I see it. If we buy personal information . . . or pull some from another database, there's never any way the customers will know about it . . . they won't ever be able to figure out . . . how can they complain?" (alterations in original)).

[51] Alessandro Acquisti, *The Economics and Behavioral Economics of Privacy*, *in* PRIVACY, BIG DATA AND THE PUBLIC GOOD: FRAMEWORKS FOR ENGAGEMENT 76, 87 (Julia Lane, e al., eds, Cambridge Univ. Press 2014) ("[A]fter an individual has released control on her personal information, she is in a position of information asymmetry with respect to the party with whom she is transacting. In particular, the subject might not know if, when, and how often the information she has provided will be used."); Paul Sholtz, *Transaction Costs and the Social Costs of Online Privacy*, FIRST MONDAY, (May 7, 2001), http://firstmonday.org/ojs/index.php/fm/article/view/859/768#note16 [https://perma.cc/9ZRE-G6JY] ("In general, a company will know a good deal more about how it uses the personal information it collects than individual consumers will."). *See generally* FRANK PASQUALE, THE BLACK BOX SOCIETY: THE SECRET ALGORITHMS THAT CONTROL MONEY AND INFORMATION (2015) (discussing how powerful interests in the online business abuse users' secrecy for profit).

[52] For example, the identity of third parties' partners who access users' data as well as the practices of collection and analysis the firm deploys can be protected under trade secrecy if the firm makes an effort to keep it confidential. *See* UNIF. TRADE SECRETS

their third party partners) possess about them from other sources, in order to estimate the risks involved in adding more information to this pool.[53] Data collection and data analytics technologies also progress at an overwhelming speed, enabling social networks to learn *more* sensitive information from *less* active information sharing by users, and obstructing users' ability to make sense of the data firms hold about them.[54]

Worse yet, as startling as it may sound, in many cases, social networks themselves do not know what information they are collecting and how they are going to use that information.[55] The decline of storage costs and the simultaneous shift to data-centric business models have prompted even small companies to collect data first, and decide what to do with it later.[56]

Not only are users unaware of firms' data management practices, but the risks involved are also not salient to them.[57]

ACT § 1(4), 14 U.L.A. at 538 (2005) (amended 1985) (defining trade secrets); *see also* Surgidev Corp. v. Eye Tech., Inc., 828 F.2d 452, 455 (8th Cir. 1987) (holding that the owner of the alleged secret "was required to take efforts 'reasonable under the circumstances' to maintain the secrecy of its customer information."); FMC Corp. v. Taiwan Tainan Giant Indus. Co., 730 F.2d 61, 62–64 (2d Cir. 1984) (per curiam) (same).

[53] *See* Mark MacCarthy, *New Directions in Privacy: Disclosure, Unfairness and Externalities*, I/S J.L. & POL'Y INFO. SOC'Y 425, 443 (2011) ("Collectors of information know what can be done with it or how it can be combined with other pieces of information to create profiles that have substantial economic value. Data subjects typically have no such knowledge and it is unreasonable to expect them to acquire it."). Note also that social networks often use cookies to track users' behavior on other websites. *See, e.g.*, *Cookies & Other Storage Technologies*, FACEBOOK, http://www.facebook.com/policies/cookies/ [https://perma.cc/4Y2Y-ZJL3].

[54] *See, e.g.*, Michal Kosinski, David Stillwell & Thore Graepel, *Private Traits and Attributes are Predictable from Digital Records of Human Behavior*, 110 PROC. NAT'L ACAD. SCIS. 5802, 5805 (2013) (finding that mere "likes" on social networks can predict users' sexual orientation, ethnicity, personality traits, political leanings, religion, personality, intelligence, substance use, satisfaction with life, and whether her parents divorced); *see also infra* notes 91–92 and accompanying text.

[55] *See* Cadie Thompson, *Companies Aim to Cash in on Your Intimate Social Data*, CNBC (Oct. 30, 2013, 2:37 PM EDT), http://www.cnbc.com/id/101151899 [https://perma.cc/E2F8-MBHT] (quoting Justin Brookman, director of consumer privacy for the Center for Democracy and Technology: "With big data there's this idea that everyone out there wants to collect it, but they don't know what to do with it. They basically say, 'We have the right to collect this data on behalf of our client and we'll figure out what to do with it later.'").

[56] Thompson, *supra* note 55. The fact that firms do not know why they collect the data is disturbing, *inter alia*, because users' consent to data use may depend on these reasons. *See, e.g.*, Jialiu Lin, Bin Liu, Norman Sadeh, & Jason I. Hong, *Modeling Users' Mobile App Privacy Preferences: Restoring Usability in a Sea of Permission Settings*, *in* PROC. OF THE TENTH SYMPOSIUM ON USABLE PRIVACY AND SECURITY at 199, 200–01 (2014) https://www.usenix.org/sites/default/files/soups14_proceedings.pdf [https://perma.cc/4KC2-NRKK] (using the purpose of the use as a parameter in evaluating the privacy performance of Android apps).

[57] *See, e.g.*, Daniel Solove, *Introduction: Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1880, 1883–88 (2013) (exploring difficulties with assessing privacy risks); Jeff Sovern, *Opting In, Opting Out, or No Options at All: The Fight for Control of Personal Information*, 74 WASH. L. REV. 1033, 1052–53 (1999) (discussing problems with assessing privacy costs); Richard Warner, *Undermined Norms: The Corrosive Effect of*

Privacy is a "credence good," the qualities of which cannot be properly assessed.[58] Users often do not know what it is that they are giving up and what value their data entails.[59] Consider also that users' imagination is restricted to familiar risks. For example, they may understand that they subject themselves to targeted ads on the social networking website, but miss the fact that their data is stored and analyzed, and is then shared with data brokers and unaffiliated third parties,[60] and may be put to unpredictable uses in the future.[61]

But merely fixing information and saliency problems would be insufficient (if at all possible). Users are not likely to *act* upon the information, even when the facts and risks are known to them. A main reason for that is that users are subject to various lock-in effects. Consider network effects.[62] The user side of the social media platform is characterized by strong network effects, because more users on the network provide more people to interact with, and thus increase the value of the network for all users.[63] Such network effects do not occur on the advertisers' side

---

Information Processing Technology on Informational Privacy, 55 ST. LOUIS L.J. 1047, 1084–86 (2011) (questioning the concept of consent as a privacy safeguard).

[58] *See generally* Michael R. Darby & Edi Karni, *Free Competition and the Optimal Amount of Fraud*, 16 J.L. & ECON. 67, 68–69 (1973) (distinguishing "credence goods" and the "credence qualities of goods" as qualities which "cannot be [easily] evaluated in normal use"); Uwe Dulleck & Rudolf Kerschbamer, *On Doctors, Mechanics, and Computer Specialists: The Economics of Credence Goods*, 44 J. ECON. LIT. 5, 5–6 (2006) ("Goods and services where an expert knows more about the quality a consumer needs than the consumer himself are called credence goods.").

[59] *See* Jan Whittington & Chris Jay Hoofnagle, *Unpacking Privacy's Price*, 90 N.C. L. REV. 1327, 1328 (2012) (stating that individuals have difficulty in determining the value of the data they are trading and the costs to which they expose themselves).

[60] *See* STAFF OF S. COMM. ON COM., SCI. & TRANSP., 113TH CONG., A REVIEW OF THE DATA BROKER INDUSTRY: COLLECTION, USE, AND SALE OF CONSUMER DATA FOR MARKETING PURPOSES 1 (2013) (reporting that established data brokers play a key role in the market for consumer data).

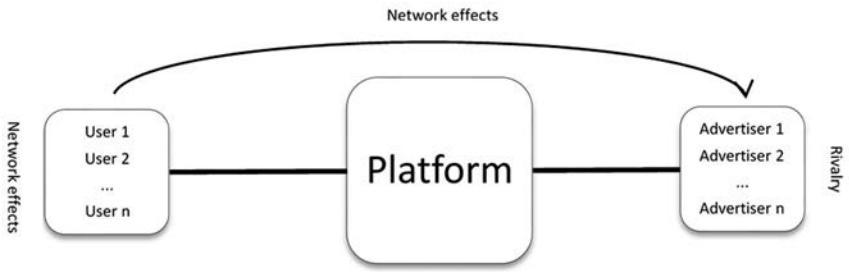
[61] *See, e.g.*, *What Do Your Social Media Posts Reveal About Your Health?*, KNOWLEDGE@WHARTON (Apr. 25, 2016) http://knowledge.wharton.upenn.edu/article/what-do-your-social-media-posts-reveal-about-your-health/ [https://perma.cc/M3AP-SCVM] (showing how an analysis of social media posts can later be used to learn of health conditions users may have); *see also* Ted Ullyot, *Facebook Releases Data, Including All National Security Requests*, FACEBOOK (June 14, 2013), http://newsroom.fb.com/News/636/Facebook-Releases-Data-Including-All-National-Security-Requests [https://perma.cc/Z8D6-BD99] (showing how users' data may be shared with non-commercial bodies, such as the government); Kosinski et al., *supra* note 54.

[62] *See generally* Michael L. Katz & Carl Shapiro, *System Competition and Network Effects*, 8 J. ECON. PERSP. 93 (1994) (discussing the economics of network effects).

[63] Alexandra Gebicka & Andreas Heinemann, *Social Media & Competition Law*, 37 WORLD COMPETITION L. & ECON. REV. 149, 161 (2014); *see also* OZ SHY, THE ECONOMICS OF NETWORK INDUSTRIES 3 (Cambridge Univ. Press, 2004) (explaining that the utility of a network product "is affected by the number of people using similar or compatible products."); Miguel Rato & Nicholas Petit, *Abuse of Dominance in Technology-Enabled Markets: Established Standards Reconsidered?*, 9 EUR. COMPETITION J. 1, 4 (2013) (discussing Metcalfe's Law, according to which the total value of a network to users is proportional to the square of the total user count).

of the market. In fact, advertisers are rivals to one another, as they compete among themselves for advertisement space.[64] *See Figure 2*. The network effects among users bind users to the network and discourage abandonment of the network. In contrast, the rivalry between advertisers on the network negates such an effect on the advertisers' side of the platform. This asymmetry tilts social networks' incentives towards satisfying advertisers, who are more likely to otherwise shift to competitors.

Figure 2



Network effects are reinforced by switching costs, which are particularly high for social media users.[65] Indeed, shifting to a new network implies not only wasting time on rebuilding digital identities and reestablishing networks,[66] but also an inferior experience for users, so long as their contacts remain in the "old" service. What is more, information that has been provided on the former service may not be fully deleted upon switching to a

---

[64] *See, e.g.*, Giacomo Luchetta, *Is the Google Platform a Two-Sided Market?*, 10 J. COMPETITION L. & ECON., 185, 202 (2013) (describing the internal bidding system on online platforms, in particular on Google). Indirect network effects may exist also between the user side of the network and its advertisers' side, namely—the higher the number of users, the more lucrative the platform for advertisers. This effect is produced because a large number of users promises a broader audience for targeted advertisements. It can also be argued that indirect network effects exist between advertisers and users because users would prefer to see increasingly diverse advertisements. There is, however, little proof that advertisements are a desired feature of social networking for users.

[65] *See generally* Joseph Farrell & Paul Klemperer, *Coordination and Lock-In: Competition with Switching Costs and Network Effects*, *in* 3 HANDBOOK OF INDUSTRIAL ORGANIZATION 1970 (Mark Armstrong & Robert H. Porter eds., 2007) (discussing the competitive effects of switching costs).

[66] *See* FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: A PROPOSED FRAMEWORK FOR BUSINESSES AND POLICYMAKERS 32 (2010), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-bureau-consumer-protection-preliminary-ftc-staff-report-protecting-consumer/101201privacyreport.pdf [https://perma.cc/34WR-WGSJ] [hereinafter FTC 2010 REPORT] ("[A] consumer who 'walks away' from a social networking site because of privacy concerns loses the time and effort invested in building a profile and connecting with friends.").

substitute.[67] This represents a "past action" catch: users may stay with the network even if they are dissatisfied with its privacy standards, simply because returning to anonymity is not an option, and switching would only duplicate the number of players who hold information about them.[68] Users are also not likely to switch because social networks are to a large extent "experience goods"—difficult to judge without actual use.[69] Thus, once a user has begun using a platform, she would find it difficult to even assess the alternatives. On top of all that, users face collective action and other coordination problems that prevent them from negotiating for better privacy terms.[70] Paul Ohm has cautioned that lock-in effects can be used strategically by firms, by way of offering robust privacy safeguards initially and changing them unfavorably after users are locked in.[71]

Some commentators have also observed that users do not have much of a choice, but to own a social media account and

---

[67] *See, e.g.*, *Privacy Policy*, LINKEDIN, https://www.linkedin.com/legal/privacy-policy [https://perma.cc/YQP4-KYEE] ("We retain your personal data even after you have closed your account if reasonably necessary to comply with our legal obligations (including law enforcement requests), meet regulatory requirements, resolve disputes, maintain security, prevent fraud and abuse, enforce our User Agreement, or fulfill your request to 'unsubscribe' from further messages from us. We will retain de-personalized information after your account has been closed."). Even social networks that do provide a full delete option may keep information that relates to other users who select to maintain it. *See, e.g.*, *How Do I Permanently Delete My Facebook Account?*, FACEBOOK HELP CTR., https://www.facebook.com/help/www/224562897555674?helpref=faq_content [https://perma.cc/6X5R-PX5E] (noting that "[s]ome information, like messages you sent to friends, may still be visible to them after you delete your account. Copies of messages you have sent are stored in your friends' inboxes.").

[68] Considering that most users join a social network when they are young and less sensitive to privacy risks (and risks generally), users' choices may reflect past preferences, if anything. *See, e.g.*, Jacqueline Howard, *What's the Average Age When Kids Get a Social Media Account?*, CNN (June 22, 2018, 2:22 PM GMT) https://edition.cnn.com/2018/06/22/health/social-media-for-kids-parent-curve/index.html [https://perma.cc/W958-4AMF]. The Right to be Forgotten, fostered by the European Commission, provides a partial solution. *See supra* note 40 art. 17. Similarly, a recent California law allows minors to erase content they post. *See* CAL. BUS. & PROF. CODE §§ 22580–22582 (West 2019).

[69] *See* Phillip Nelson, *Information and Consumer Behavior*, 78 J. POL. ECON. 311, 312–14 (1970) (contrasting experience goods with search goods).

[70] *See*, *e.g.*, SAMUEL BOWLES, MICROECONOMICS 127–66 (Princeton Univ. Press 2004) (exploring when players are better off when taking similar actions); MANCUR OLSON, THE LOGIC OF COLLECTIVE ACTION: PUBLIC GOODS AND THE THEORY OF GROUPS 33–36, 43–52, 124–31 (4th ed., Harvard Univ. Press 1974). Occasionally, social network users were able to push back on planned data use. *See, e.g.*, David Coursey, *After Criticism, Facebook Tweaks Friends List Privacy Options*, PC WORLD (Dec. 10, 2009, 6:17 PM PT), http://www.pcworld.com/article/184418/After_Criticism_Facebook_Changes_Friend_List_Privacy_Options.html [http://perma.cc/BBG9-HV4D] (reporting that following users' outrage, Facebook gave users the opportunity to protect their Friends List from public view); Kashmir Hill, *Instagram Cowed by Privacy Outrage, Won't Put Photos in Ads*, FORBES (Dec. 18, 2012, 5:22 PM), http://www.forbes.com/sites/kashmirhill/2012/12/18/instagram-cowed-by-privacy-outrage-wont-put-photos-in-ads/ [https://perma.cc/Y97U-MSF9] (reporting that users' indignation caused Instagram to reverse a planned privacy change).

[71] Ohm, *supra* note 45, at 922.

submit to the terms the network sets.[72] In a world where online presence is unescapable, social networks provide an online presence that individuals can control.[73] What is more, avoiding social media is becoming increasingly impractical. Increasingly, potential employers, dating partners, university admission committees and others use social media to learn about candidates.[74] Access to certain services is also becoming conditioned upon possessing a social media account.[75]

But even if opting out of social media were a valid "choice," various cognitive biases induce users to make disinterested choices in this regard. These biases include, *inter alia*, optimism bias,[76] limited foresight perspective,[77] crowd

---

[72] *See, e.g.*, Strandburg, *supra* note 31, at 164–65 (discussing the "take it or leave it" nature of online privacy deals). *See generally* JOSEPH TUROW, MICHAEL HENNESSY & NORA DRAPER, THE TRADEOFF FALLACY: HOW MARKETERS ARE MISREPRESENTING AMERICAN CONSUMERS AND OPENING THEM UP TO EXPLOITATION 3 (2015) (explaining users' putting up with privacy-invasive practices not by a theory of willful choice, but by a theory of resignation, namely, a belief that an "undesirable outcome is inevitable" and a feeling of helplessness to change it).

[73] *See* Mitja D. Back et al., *Facebook Profiles Reflect Actual Personality, Not Self-Idealization*, 21 PSYCHOL. SCI. 372, 372 (2010) (noting that social networking sites "have become integrated into the milieu of modern-day social interactions"). Of course, technically, "Nobody's got to use the Internet, at all", as some rhetoricians like to point out. Kate Cox, *Killing Privacy Is Fine Because "Nobody's Got to Use the Internet," House Rep Says*, CONSUMERIST (Apr. 17, 2017, 11:38 AM EDT), https://consumerist.com/2017/04/17/killing-privacy-is-fine-because-nobodys-got-to-use-the-internet-house-rep-says/ [https://perma.cc/N499-96FL] (quoting Wisconsin Rep. Jim Sensenbrenner) (internal quotation marks omitted).

[74] *See* Alessandro Acquisti & Christina M. Fong, An Experiment in Hiring Discrimination via Online Social Networks 2 (July 17, 2015) (unpublished manuscript), http://ssrn.com/abstract=2031979 [https://perma.cc/MSD5-C96T] (finding that employers use social media to screen applicants, including on discriminatory features); *see also* Martha C. White, *More Colleges are Cyber-Stalking Students During the Admissions Process*, TIME (Mar. 9, 2016), http://time.com/money/4252541/colleges-facebook-social-media-students-admissions/ [https://perma.cc/23CK-RW2B] (reporting a survey where 45% of admissions officers reported searching online for school applicants).

[75] Alessandro Acquisti et al., *What Is Privacy Worth?* 42 J. LEGAL STUD. 249, 257 (2013) ("[I]n some cases, consumers can get access to certain goods or services (such as listening to music on Spotify or commenting on news stories on the *Los Angeles Times*'s Web site) only through a social network that tracks their behavior and links it to their actual identities (Facebook)." (footnotes omitted)).

[76] *See generally* TALI SHAROT, THE OPTIMISM BIAS: A TOUR OF THE IRRATIONALLY POSITIVE BRAIN (2011) (explaining optimism bias as an underestimation of risks); Christine Jolls et al., *A Behavioral Approach to Law and Economics*, 50 STAN. L. REV. 1471, 1524 (1998); Barbara Luppi & Francesco Parisi, *Beyond Liability: Correcting Optimism Bias Through Tort Law*, 35 QUEEN'S L.J. 47, 48 (2009); Neil D. Weinstein, *Optimistic Biases About Personal Risks*, 246 SCIENCE 1232 (1989); Neil D. Weinstein, *Unrealistic Optimism About Future Life Events*, 39 J. PERSONALITY & SOC. PSYCHOL. 806 (1980).

[77] *See* Philippe Jehiel & Andrew Lilico, *Smoking Today and Stopping Tomorrow: A Limited Foresight Perspective* 4–8 (CESifo, Working Paper No. 2603, 2009) (explaining limited foresight as overvaluing immediate over long term consequences); Diana I. Tamir & Jason P. Mitchell, *Disclosing Information About the Self Is Intrinsically Rewarding*, 109 PROC. NAT'L ACAD. SCI. 8038, 8038 (2012), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3361411/pdf/pnas.201202129.pdf [https://perma.cc/G26F-WKPT] (showing how sharing information provides immediate gratification).

bias,[78] "bounded rationality,"[79] loss aversion,[80] and the lure of "free."[81] Social media has also become addictive,[82] and its user interface is carefully designed to imitate and revoke intimacy, coziness, safety, and trust, in order to induce sharing.[83] Self-control bias plays a significant role as well.[84] Leading social networks moved to allow users to restrict the visibility of their content to other users.[85] This move produced a sense of control over information visibility and obscured the fact that the social network itself is a "silent listener" to all the communications on the network.[86] These—and other[87]—biases allow firms to exploit the gap between privacy choices that a rational user would make and those made by an actual user with predictable flaws.[88] In

---

[78] *See* Alessandro Acquisti, Leslie John & George Loewenstein, *The Impact of Relative Standards on the Propensity to Disclose*, 49 J. MKTG. RES. 160, 172 (2012) (finding that individuals are more likely to disclose information if told that others have done the same).

[79] Acquisti, *Privacy in Electronic Commerce*, *supra* note 51, at 22 ("[B]ounded rationality refers to the inability to calculate and compare the magnitudes of payoffs associated with various strategies the individual may choose in privacy-sensitive situations. It also refers to the inability to process all the stochastic information related to risks and probabilities of events leading to privacy costs and benefits.").

[80] *See* Daniel Kahneman & Amos Tversky, *Prospect Theory: An Analysis of Decision Under Risk*, 47 ECONOMETRICA 263, 263 (1979) (defining loss aversion as the disproportionate weight that people tend to place on losses relative to gains).

[81] *See* Hoofnagle & Whittington, *supra* note 5, at 628.

[82] *See* Manya Sleeper et al., *I Would Like To . . . , I Shouldn't . . . , I Wish I . . . : Exploring Behavior-Change Goals for Social Networking Sites*, *in* 18 ACM CONFERENCE ON COMPUTER SUPPORTED COOPERATIVE WORK & SOCIAL COMPUTING 1058, 1061 (2015) (finding that 31% of survey participants wish to use their social networking less; 41% on Facebook).

[83] Thomas Hughes-Roberts & Elahe Kani-Zabihi, *On-Line Privacy Behavior: Using User Interfaces for Salient Factors*, 2 J. COMPUTER & COMMS. 220, 227–28 (2014) (exploring the role of "persuasive technology" social media use in triggering sharing); *see also* SIVA VAIDHYANATHAN, THE GOOGLIZATION OF EVERYTHING (AND WHY WE SHOULD WORRY) 84 (2011) (discussing, in the context of Google, how "in the end, policies matter less than design choices. With Google, the design of the system rigs it in favor of the interests of the company and against the interests of users.").

[84] Laura Brandimarte et al., *Misplaced Confidences: Privacy and the Control Paradox*, 4 SOC. PSYCHOL. & PERSONALITY SCI. 340, 345 (2012) (finding that the more perceived control users have over sharing, the less cautious they become).

[85] On the privacy harms social media creates between users, *see* Grimmelmann, *supra* note 38, at 1164–78.

[86] Stutzman et al., *supra* note 1, at 9 ("[P]erceptions of control over personal data and misdirection of users' attention have been linked in the literature to increases in disclosures of sensitive information to strangers." (internal citations omitted)); Andrew Besmer & Heather Richter Lipford, *Users' (Mis)Conceptions of Social Applications*, GRAPHICS INTERFACE 2010 63, 70 https://pdfs.semanticscholar.org/b5e4/fb0eec3457cacf24ddfa0e6d38e98975edec.pdf [https://perma.cc/9Q9E-Q6R7] ("[P]rivacy concerns are centered around sharing data with other people on the social network, with almost no understanding of the data sharing that occurs with the application developers.").

[87] *See, e.g.*, Ted O'Donoghue & Matthew Rabin, *Choice and Procrastination*, 116 Q. J. ECON. 121, 125–26 (2001) (discussing context-based decision-making and hyperbolic discounting); Holland, *supra* note 37, at 893–94 (applying theories from behavioral economics to the privacy context).

[88] *See* Ryan Calo, *Digital Market Manipulation*, 82 GEO. WASH. L. REV. 995, 999 (2014); *see also* Sam Levin, *Facebook Told Advertisers it Can Identify Teens Feeling 'Insecure' and 'Worthless'*, GUARDIAN (May 1, 2017, 3:01 PM EDT), https://

Oren Bar-Gill's terminology, these disinterested choices form a behavioral market failure—"a persistent consumer mistake that causes substantial welfare loss."[89]

Worse yet, even when users do make acceptable privacy decisions for themselves, privacy decisions that they make individually impose externalities on other users and on society as a whole.[90] The most obvious externality occurs when information voluntarily disclosed by one individual is used to infer information about others.[91] Improved data science methodologies allow social networks to tease out intimate information about users from the online behavior of their contacts ("friends").[92] For example, an individual whose contacts are involved in a certain political party, gay community, or a "foodies" forum (or whose behavior shows similarities to members of such groups) may be flagged as having those traits even if the user herself has selected to remain silent on such matters.[93] In other words, data collection on social networks produces exponential externalities by exposing to risks more than just the individual who is directly tracked.[94]

---

www.theguardian.com/technology/2017/may/01/facebook-advertising-data-insecure-teens [https://perma.cc/2N8U-CSEV].

[89] Oren Bar-Gill & Franco Ferrari, *Informing Consumers about Themselves*, 3 ERASMUS L. REV. 93, 119 (2010) (discussing use pattern mistakes consumers make); *see also* Oren Bar-Gill, *Competition and Consumer Protection: A Behavioral Economics Account*, *in* THE PROS AND CONS OF CONSUMER PROTECTION 12–43 (Sten Nyberg, ed., Swedish Competition Auth. 2012); Cass R. Sunstein, *The Storrs Lectures: Behavioral Economics and Paternalism*, 122 YALE L.J. 1826, 1842–52 (2013) (identifying present bias and time inconsistency, ignoring shrouded attributes, unrealistic optimism, and probability problems as forms of behavioral market failure).

[90] This point has traditionally been overlooked by lawmakers in the United States. *See* JAMES P. NEHF, OPEN BOOK: THE FAILED PROMISE OF INFORMATION PRIVACY IN AMERICA 4 (2012) ("In the United States, information privacy has historically been defined as an individual concern rather than a general societal value or a public interest problem.").

[91] *See* Grimmelmann, *supra* note 38, at 1150, 1174–75; *see also* Dennis D. Hirsch, *Protecting the Inner Environment: What Privacy Regulation Can Learn from Environmental Law*, 41 GA. L. REV. 1, 23 (2006) (discussing how privacy-related externalities are similar to environmental externalities).

[92] *See, e.g.*, Authorization and Authentication Based on an Individual's Social Network, U.S. Patent No. 9,391,971 B2 (filed May 29, 2014) (issued July 12, 2016) ("In a fourth embodiment of the invention, the service provider is a lender. When an individual applies for a loan, the lender examines the credit ratings of members of the individual's social network who are connected to the individual through authorized nodes. If the average credit rating of these members is at least a minimum credit score, the lender continues to process the loan application. Otherwise, the loan application is rejected.").

[93] *See* MacCarthy, *supra* note 53, at 445–46 (noting that social networks learn about users from others mentioning their names, "tagging" them in photos, writing to or about them, or inviting them to events); *see also* Matthew Moore, *Gay Men 'Can Be Identified by Their Facebook Friends'*, TELEGRAPH (Sept. 21, 2009, 10:45 AM BST), http://www.telegraph.co.uk/technology/facebook/6213590/Gay-men-can-be-identified-by-their-Facebook-friends.html [https://perma.cc/T2NW-2N3S].

[94] *See* MacCarthy, *supra* note 53, at 443 ("The idea is that individual choice in this area would lead, in a piecemeal fashion, to the erosion of privacy protections that are the foundation of the democratic regime, which is the heart of our political system.

Clearly, better privacy competition between social networks could have alleviated many of these problems. Yet privacy competition is rarely the case on social media, for two main reasons. First, social networks face fierce competition on advertisers.[95] As long as the "economy of free" controls online services, digital market players eschew charging users for services, and instead leverage data for transactions with third parties. This phenomenon, labeled by Paul Ohm and others "the 'Google envy' effect,"[96] induces a rush to the bottom in terms of privacy protection, as firms are compelled to constantly race to collect and analyze data on their users.[97] To stay ahead, social networks must exploit to the fullest the scope of personal information they retain on individuals, rather than to offer stronger privacy protection that would limit their use of users' data.[98] Of course, social networks need to compete for users too, but this need is attenuated due to the lock-in effects and the other market failures discussed in this Part, and generally revolves around features other than privacy, such as network size and usability.[99]

Second, powerful network effects and other lock-in effects that this Part discussed have made the market power of dominant social networks more durable and have spurred the creation of monopolies in the social networking space.[100] Besides

---

Individuals are making an assessment—at least implicitly—of the advantages and disadvantages to them of sharing information. They are determining that information sharing is, on balance, a net gain for them. But the aggregate effect of these decisions is to erode the expectation of privacy and also the role of privacy in fostering self-development, personhood, and other values that underlie the liberal way of life." (footnotes omitted)).

[95] *See* Ohm, *Branding Privacy*, *supra* note 45, at 927 ("Many companies are actively reshaping their business models to try to profit from customer secrets, and by doing this, they find themselves in a large, diverse market, squaring off against competitors from what used to be non-competitive market segments.").

[96] Paul Ohm, *The Rise and Fall of Invasive ISP Surveillance*, 2009 U. ILL. L. REV. 1417, 1426 (2009) ("Providers have what some have called 'Google envy.' Google has demonstrated how to grow rapidly by monetizing user behavior, in their case by displaying advertisements matching a users' recent search queries." (footnotes omitted)).

[97] *See* Grunes, *supra* note 39, at 1118 ("[A]ntitrust law does not regard this form of competition as particularly worthy of protection, including the fact that the competition is on the free side and not the paying side of the market.").

[98] Social networks possess other competitive advantages for marketers at the expense of user privacy. As discussed herein, they typically forbid anonymous use, they can use information about past users, and they can infer information about users who have not revealed information voluntarily. *See infra* Section III.C; *see also* Grimmelmann, *supra* note 38, at 1150, 1174–75.

[99] *See, e.g.*, Russell Korobkin, *Bounded Rationality, Standard Form Contracts, and Unconscionability*, 70 U. CHI. L. REV. 1203, 1206 (2003) ("Because buyers are boundedly rational rather than fully rational decisionmakers, when making purchasing decisions they take into account only a limited number of product attributes and ignore others.").

[100] *See generally* Nolte et al., *supra* note 31 (illustrating the dominant position of some social networks). Firms also maintain their dominant positions by buying out

potential antitrust concerns, this dynamic also feeds the disincentive of social networks to improve their privacy offerings to users and discourage the creation of a privacy market.[101]

The reality under the current regime is inefficient. Firms' incentive to adopt a less robust privacy regime stems not from higher gains data collection yields relative to the harms it generates for users, which would mean that this practice passed a real market test. Rather, this effect is achieved because firms realize that their privacy practices will not shift demand even if they *do* reduce users' welfare. Firms therefore conclude that their best strategy is to pursue higher gains from users' information, *regardless* of the harms this strategy inflicts. As Brian Holland put it, under the extant regime, social networks are "able to internalize the benefits of personal data while externalizing most of the costs."[102]

II. THE PROPOSAL

This Part of the article will delineate the proposal to harness executive pay to improve data management practices in social networking enterprises. My vision is to add another component to the classic executive contract, which is typically composed of a fixed wage and a performance bonus. This new component, the "privacy performance" pay, would depend on a privacy-protection score.

The first Section below explains the rationale to manipulate executive compensation in this context. The second Section details the mechanism for the implementation of the proposal and the steps necessary to make it work efficiently. The third Section explores the benefits this model encompasses and shows that adding the proposed incentive payment is welfare improving.

A. Why Executive Compensation?

Since the 1990s, performance-based compensation has become the leading structure of executive compensation.[103] As

---

competitors, such as the recent purchases of WhatsApp and Instagram by Facebook. *See, e.g.*, Olson, *supra* note 45 (discussing aspects of the WhatsApp acquisition).

[101] *See supra* note 99 and accompanying text.

[102] *See* Holland, *supra* note 37, at 904.

[103] Performance-based compensation is also exempted from the prohibition of deduction of executive compensation in excess of $1 million. *See* I.R.C. §§ 162(m)(1)–(4)(C)(2012) ("Certain excessive employee remuneration . . . no deduction shall be allowed under this chapter for applicable employee remuneration with respect to any covered employee to the extent that the amount of such remuneration for the taxable year with respect to such employee exceeds $1,000,000," unless certain performance based goals apply.); *see also id.* § 280G (regulating Golden Parachute Payments). After

their name implies, "Pay for Performance" programs link executive compensation to the firm's economic performance. Normally, compensation deals are composed of a fixed wage and a bonus that depends on the firm's stock performance. The idea behind performance-based compensation is to align the interests of executives with that of shareholders, in order to maximize stock value.[104]

Pay for Performance schemes have been subject to criticisms for two main reasons. First, scholars have argued that such schemes are ineffective in achieving their goal to promote shareholders' interests.[105] Second, critics observed that these schemes motivate executives to externalize costs to society in the pursuit of boosting the share price.[106]

These flaws of the Pay for Performance model strongly manifest themselves in the context of social media privacy. As discussed below, executive compensation packages create an agency problem, because they motivate executives to pursue short-term profits at the expense of the shareholders' long-term interest in maintaining trust in the system.[107] Such compensation schemes also encourage social media executives to externalize the costs associated with overexploitation of users' data to users and to society as a whole. Augmenting the standard executive compensation deal in social media firms with a payment that reflects the firm's level of privacy protection would address both these inefficiencies.

Consider first how manipulating executive compensation can tackle the agency problem between executives and long-term shareholders. Despite current users' fatigue, privacy concerns may eventually create a chilling effect on the use of social media.[108]

---

the recent financial crisis, the Dodd-Frank Act of 2010 aimed to embed "pay for performance" firmly into federal law. *See* Dodd-Frank Wall Street Reform and Consumer Protection Act, Pub. L. No. 111-203, 124 Stat. 1376, 1899–1907 (2010).

104 Charles M. Yablon, *Bonus Questions: Executive Compensation in the Era of Pay for Performance*, 75 NOTRE DAME L. REV. 271, 273 (1999) ("The theory of pay for performance is that shareholders benefit when management compensation . . . is dependent on a high level of corporate performance.").

105 *See, e.g.*, Steven A. Bank & George S. Georgiev, *Paying High for Low Performance* 100 MINN. L. REV. HEADNOTES 14, 19 (2016) (showing that there is no correlation between the compensation executives receive and the actual state of their firm); Lucian Arye Bebchuk, Jesse M. Fried & David I. Walker, *Managerial Power and Rent Extraction in the Design of Executive Compensation*, 69 U. CHI. L. REV. 751, 752 (2002) (criticizing the prevalent U.S. executive compensation model); Meredith M. Stead, *How Incentive Pay for Executives Isn't—and What We Can Do About It*, 80 N.Y.U. L. REV. 722, 724 (2005) (arguing that both equity and non-equity based compensation in its current form fail to effectively tie compensation to performance).

106 *See infra* notes 126–127 and accompanying text.

107 *See infra* note 108 and accompanying text.

108 *See* FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS 8 (2012)

While using social media extensively, users *do* find social media privacy practices objectionable. A recent study by Pew Center found that eighty percent of social networking users said that they were concerned that some of the information they share on social networking sites might be accessed by third parties like advertisers or businesses without their knowledge.[109] In another study at the University of Pennsylvania, ninety-one percent of respondents disagreed (seventy-seven percent of them strongly) that "[i]f companies give me a discount, it is a fair exchange for them to collect information about me without my knowing."[110]

Users also employ a range of strategies in an attempt to protect their privacy. Studies documented privacy-seeking behaviors such as adopting of technical protections, arranging privacy settings within social media sites, using fake profiles, and practicing "self-censorship and withdrawal of content."[111] Some reports also show that Facebook users have shifted from sharing

("[Privacy protections] not only will help consumers but also will benefit businesses by building consumer trust in the marketplace."); *Data Privacy Is a Major Concern for Consumers,* TRUSTARC BLOG (Jan. 28. 2015), http://www.truste.com/blog/2015/01/28/data-privacy-concern-consumers/ [https://perma.cc/S3GK-8H73] (citing surveys that show that "[c]onsumers consider data privacy to be a hot button issue."); Leslie Harris, *The Best Practices Act of 2010 and Other Federal Privacy Legislation*, CTR. FOR DEMOCRACY & TECH. 1 (July 22, 2010), http://www.cdt.org/files/pdfs/CDT_privacy_bill_.pdf [https://perma.cc/4S7B-WL53] ("Privacy is an essential building block of trust in the digital age."); Samantha Murphy Kelly, *Facebook's Facial-Recognition Acquisition Raises Privacy Concern*s, MASHABLE (June 25, 2012), http://mashable.com/2012/06/25/facebook-facial-recognition-privac/ [https://perma.cc/ZV6M-N6CT] ("[S]ome users might exercise more caution with how they upload pictures."); John Rose et al., *The Trust Advantage: How to Win with Big Data*, BOS. CONSULTING GROUP (Nov. 6, 2013), https://www.bcgperspectives.com/content/articles/information_technology_strategy_consumer_products_trust_advantage_win_big_data/ [https://perma.cc/54S9-QFJJ] ("In order for global companies to have the greatest possible access to personal data, consumers need to trust that this information will be well stewarded.") Press Release, Carnegie Mellon Univ., Increasing Control over Release of Information Leads People to Divulge More Online, Carnegie Mellon Researchers Find (Nov. 28, 2012), https://www.cmu.edu/news/stories/archives/2012/november/nov28_informationcontrol.html [https://perma.cc/356K-JTEV].

[109] Mary Madden, *Few Feel that the Government or Advertisers Can Be Trusted*, PEW RES. CTR. (Nov. 12, 2014), http://www.pewinternet.org/2014/11/12/few-feel-that-the-government-or-advertisers-can-be-trusted/ [https://perma.cc/7PKN-BCRE].

[110] *See* Turow et al., *supra* note 72, at 3.

[111] Stutzman et al., *supra* note 1, at 10 (individuals engage in "self-censorship and withdrawal of content"); *see, e.g.*, Kevin Lewis, Jason Kaufman & Nicholas Christakis, *The Taste for Privacy: An Analysis of College Student Privacy Settings in an Online Social Network*, 14 J. COMPUTER-MEDIATED COMM. 79, 79–83; Jonathan Mayer, *Government Hacking*, 127 YALE L.J. 570, 576 ("Individuals and businesses are rapidly adopting technical protections . . . ."); danah boyd & Eszter Hargittai, *Facebook Privacy Settings: Who Cares?*, 15 FIRST MONDAY (2010), https://firstmonday.org/article/view/3086/2589 [https://perma.cc/PL64-P46X] (finding an increase in youth's practices to modify privacy settings on Facebook between 2009–2010); *see also* Michael E. Lackey & Joseph P. Minta, *The Ethics Of Disguised Identity In Social Media*, 24 ALB. L.J. SCI. & TECH. 447, 458–59 (2014) (discussing the use of disguised identities on social media); *Caveat Emptor.com*, ECONOMIST (June 30, 2012) (discussing measures for consumers to avoid personalized price discrimination).

personal, original information to sharing secondary information, such as articles and news reports.[112] Also, younger users are increasingly quitting Facebook and joining more private options, such as Snapchat and WhatsApp. Indeed, Snapchat and WhatsApp are only more private among the community of users and not in the relationships of users with the network itself; yet this trend indicates that users are not as privacy-indifferent as some would like to believe. At the end of the day, over-exploiting users' privacy may jeopardize the trust individuals have in social media and in the data-centric business model.[113]

Social networks can compensate for some decline in data sharing by tracking users' behaviors on other platforms[114] and by utilizing increasingly aggressive data analytics technologies.[115] But these strategies cannot be counted on forever, and in the long run they may exacerbate users' privacy concerns. Increasing public unrest around privacy can also prompt regulation, which will impose limitations on social networks' data practices.[116]

Granted, the risks that users would detrimentally change their sharing patterns (or that regulators would step in to protect them) will not necessarily materialize, whether due to the lock-in effects I explored in Part I or for any other reason. Yet, this is a

---

[112] Sarah Frier, *Facebook Wants You to Post More About Yourself*, BLOOMBERG TECH. (Apr. 7, 2016, 4:36 PM EDT) https://www.bloomberg.com/news/articles/2016-04-07/facebook-said-to-face-decline-in-people-posting-personal-content [https://perma.cc/HQD5-YR7K] (noting that personal sharing on Facebook has declined by 21%). Note, however, that alternative explanations for this decline include growing number of contacts Facebook users have or migration of content to other social networks. *Id.*

[113] *See* sources cited *supra* notes 108–109.

[114] *See* MacCarthy, *supra* note 53, at 500–02; *Cookies & Other Storage Technologies*, *supra* note 53. Note also that M&A strategies in the industry can allow social network to share data across platforms, such as Facebook's purchases of Instagram and WhatsApp. *See, e.g.*, Olson, *supra* note 45 (discussing aspects of the WhatsApp acquisition).

[115] *See* Kosinki et al., *supra* note 54.

[116] For possible regulations, see, e.g., Biometric Information Privacy Act (BIPA), 740 ILL. COMP. STAT. 14/5–15 (2008); Norberg v. Shutterfly, Inc., 152 F. Supp. 3d 1103, 1106 (N.D. Ill. 2015) (denying Shutterfly's motion to dismiss a case that argues that scanning a face geometry without consent is a violation of BIPA); EXEC. OFFICE OF THE PRESIDENT, CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY 7 (2012), https://www.hsdl.org/?view&did=700959 [https://perma.cc/4VMW-D7P2] (noting a consumer privacy bill of rights, enforceable codes of conduct, and increased FTC enforcement, as paths toward improved consumer data privacy); *see also* General Data Protection Regulation, *supra* note 40. In Europe, the first EU directive was drafted already in 2015. *See* Directive 95/46/EC of the European Parliament and of the Council, 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 O.J. (L 281) 31–50; *see also Protection of Personal Data*, EUROPEAN COMM'N, https://ec.europa.eu/info/aid-development-cooperation-fundamental-rights/your-rights-eu/know-your-rights/freedoms/protection-personal-data_en [https://perma.cc/GPF9-Y4KW]. The more comprehensive regulation of the GDPR was adopted in 2016. *See supra* note 40.

plausible scenario, considering the level of unease users express regarding the current state of affairs, and the early signs of change in sharing patterns.[117] Despite the plausibility of these risks, however, executives cannot be trusted to internalize and mitigate them. The first reason for that is that structuring officers' incentives to maximize shareholder value inherently encourages excessive risk taking.[118] Under this compensation framework, executives are rewarded for high performance, but are not penalized for low performance. "The asymmetry between the high rewards for success and the low [penalty for] failure" motivates executives to assume risks in the hopes of personal and corporate gain if they do not materialize.[119] In the case of social network privacy, executives are prone to take the risk of overuse of personal data for the gains the data use yields.[120] This risky attitude is intensified because contending with the long-term risk of users' trust requires sacrifices in the short-term accounting metrics, to which officers' pay is tied.[121]

There are also good reasons to believe that executives systematically underestimate the risk that users will eventually act upon privacy harms. The first reason for that is the notorious optimism bias that was mentioned above in a different context.[122] Optimism bias can make officers underestimate the likelihood that users would lose trust in the platform or that regulators would make substantial changes to the status quo. The second

---

[117] *See supra* notes 109–112 and accompanying text; *see also* HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE 7 (2010) ("As the privacy conundrum has grown in public awareness it has attracted the attention of leaders in all social sectors, including business, government, and education, as well as scholars and researchers across the disciplines.").

[118] *See* Eric D. Chason, *The Uneasy Case for Deferring Banker Pay*, 73 LA. L. REV. 923, 925 (2013) (arguing that changes for incentive-based compensation in the financial industry are crucial to curb risky behavior); Lisa M. Fairfax, *Government Governance and the Need to Reconcile Governmental Regulation with Board Fiduciary Duties*, 95 MINN. L. REV. 1692, 1696 (2011) (arguing that the current corporate compensation structures incentivized executives to take excessive risks); Jeffrey Manns, *Insuring Against a Derivative Disaster: The Case for Decentralized Risk Management*, 98 IOWA L. REV. 1575, 1577 (2013) (proposing a strategy for decentralized risk management to tackle financial bubbles).

[119] Chason, *supra* note 118, at 926.

[120] *See* MARY MADDEN & LEE RAINIE, PEW RES. CTR., AMERICANS' ATTITUDES ABOUT PRIVACY, SECURITY AND SURVEILLANCE 8 (2015), http://www.pewinternet.org/files/2015/05/Privacy-and-Security-Attitudes-5.19.15_FINAL.pdf [https://perma.cc/JVT8-ZCE9] (noting that "69% of adults say they are not confident that records of their activity records maintained by the social media sites that they use will remain private and secure.").

[121] The pursuit of short-term value can also be desired by short-term shareholders, who may influence executives to take this path. *See* COLIN MAYER, FIRM COMMITMENT: WHY THE CORPORATION IS FAILING US AND HOW TO RESTORE TRUST IN IT 185–86 (2013) (explaining how short-term shareholders press managers to take steps that advance their interests).

[122] *See supra* note 76.

reason is that corporate officers appear to value privacy less than most people, and thus may underappreciate the magnitude of users' privacy concerns.[123] New research by Victoria Schwartz argues that extensive corporate disclosure requirements as well as media interest in the personal lives of corporate executives sort the pool of corporate executives towards individuals who do not highly value privacy.[124] Clearly, these are two different kinds of privacy: classic privacy issues of media attention to an individual, and processing a massive amount of seemingly mundane data. Yet the relative indifference of executives to sharing information about themselves may blind them from realizing that they overexploit users' personal information and drive them to downplay the risk that users will change their behavior as a result.[125]

Consider now how including a privacy-based pay component in compensation deals can curb executives' incentives to externalize privacy costs. As mentioned above, executive compensation packages have traditionally been designed to tackle the agency problem between officers and shareholders, namely, the concern that officers would advance their own interests over those of shareholders.[126] Consequently, executive compensation packages are designed to align executives' incentives with those of shareholders, and they typically disregard value or disvalue for non-shareholder stakeholders, including the privacy interests of the firm's users.[127]

In fact, privacy is the most natural victim of Pay for Performance programs in the context of social media. Beyond concerns of compliance and legal risks, privacy has little effect on the stock price, because users rarely act on privacy harms, at

---

[123] *See* Victoria L. Schwartz, *Corporate Privacy Failures Start at the Top*, 57 B.C. L. REV. 1693, 1712 (2016).

[124] *Id.*

[125] Similarly, the well-known phenomenon of conformism might make executives conform with industry norms or with the sales department's wishes. *See, e.g.*, James Fanto, *Whistleblowing and the Public Director: Countering Corporate Inner Circles*, 83 OR. L. REV. 435, 462 (2004).

[126] *See supra* note 104.

[127] The question of whether firms should also be responsible to non-shareholder-stakeholders is debated in the scholarship. The extant law, at least that of executive compensation, reflects the approach that shareholder value should be the firm's ultimate aim. *See, e.g.*, FRANK H. EASTERBROOK & DANIEL R. FISCHEL, THE ECONOMIC STRUCTURE OF CORPORATE LAW 38 (1991) ("[M]aximizing profits for equity investors assists the other 'constituencies' automatically."); John C. Coffee, Jr., *A Theory of Corporate Scandals: Why the USA and Europe Differ*, 21 OXFORD REV. ECON. POL'Y 198, 202 (2005); Henry Hansmann & Reinier Kraakman, *The End of History for Corporate Law*, 89 GEO. L.J. 439, 439 (2001) ("There is no longer any serious competitor to the view that corporate law should principally strive to increase long-term shareholder value.").

least for now.[128] Exploiting data to improve ad-targeting may actually appear to *boost* performance, despite the long term risks discussed herein, because advertisers are willing to pay more for well-targeted ads.[129] Because, as explored above, executives are not likely to fear that any of this is going to change, their focus is on exploiting users' data to the fullest, regardless of the harms users may incur as a result.

Executives' incentive to disregard user privacy has empirical support. Studies found that "executives eschew[] any responsibility . . . to proactively identify and address privacy issues. Aside from complying with laws prescribing corporate behavior, executives felt their duty was to maintain maximum flexibility over data use to ensure profitability."[130] Clearly, compliance does create *some* incentives to internalize privacy, whether via FTC fines or the European General Data Protection Regulation (GDPR), which can affect the behavior of multinational firms.[131] Yet, compliance alone does not ensure adequate privacy protection, and smaller firms are not even likely to invest in compliance.[132]

Redesigning executive compensation to include privacy considerations would expose executives to the risks both users and firm shareholders are bearing due to the trade in users' data. This move can thus both remediate externalities and reduce the managerial agency costs this Part discussed.[133]

B. The Mechanism

Part of the compensation of executives in social networks should be determined by the quality of the privacy protection

---

[128] *See supra* Part I.

[129] *See* Grunes, *supra* note 39, at 1110–11 (noting that personal information allows advertisers to target their market and to measure effectiveness).

[130] Bamberger & Mulligan, *New Governance*, *supra* note 50, at 499. *But see* Bamberger & Mulligan, *Privacy on the Books*, *supra* note 20, at 272 (describing interviews with Chief Privacy Officers within firms who describe a shift of the privacy discussion from compliance to risk-management).

[131] *See* sources cited *supra* notes 25, 40.

[132] *See* Birnhack & Elkin-Koren, *supra* note 35, at 380 (analyzing companies' compliance with privacy laws).

[133] Preventing externalities and furthering the interests of long-term shareholders can go hand in hand. *See, e.g.*, Lisa M. Fairfax, *The Rhetoric of Corporate Law: The Impact of Stakeholder Rhetoric on Corporate Norms*, 31 J. CORP. L. 675, 702 (2006) ("[P]roponents of the long-term view of shareholder primacy would contend that such a view accommodates non-shareholder issues. . . . because 'stakeholder' concerns, such as giving money to charity or behaving responsibly towards employees and customers, inure to the benefit of shareholders in the long-term." (footnotes omitted)); Virginia Harper Ho, *"Enlightened Shareholder Value": Corporate Governance Beyond the Shareholder-Stakeholder Divide*, 36 J. CORP. L. 59, 62 (2010) (arguing that attention to stakeholder interests leads to long-term shareholder wealth); *see also infra* Section III.B.3.

that their firm applies. To achieve this, there should be a mechanism of privacy rating for social networking firms. Privacy officers in the firm would operationalize this model, and the firm's compensation committee would factor this score into executive compensation packages.

1. The Standard for Privacy

The first—and most prominent—challenge of the model is how to measure the quality of data protection social networking firms employ. The analysis of this challenge is guided by two assumptions. The first is that privacy is neither a static nor a homogeneous concept. Privacy is a moving target, constantly evolving with technology, market trends, and social expectations.[134] Privacy preferences are also heterogeneous, namely some individuals value privacy more than others.[135] Second—and notably, though often overlooked—too much privacy can be as bad as too little. Among other things, too much privacy can curb innovation (such as in the area of data analytics), increase access prices to social networks (that are mostly free

---

[134] *See* Fred H. Cate & Robert Litan, *Constitutional Issues in Information Privacy*, 9 MICH. TELECOMM. & TECH. L. REV. 35, 61 (2002) ("The public's expectations of privacy are changing, as are the many influences that shape those expectations, such as technology, law, and experience."); Adam Thierer, *A Framework for Benefit-Cost Analysis in Digital Privacy Debates*, 20 GEO. MASON L. REV. 1055, 1101–02 (2013) (describing a resistance, adaptation, assimilation cycle towards privacy-related technologies); Jake Nevrla, Commentary, *Voluntary Surveillance: Privacy, Identity and the Rise of Social Panopticism in the Twenty-First Century*, 6 COMM-ENTARY 5, 5–6 (2010), https://cola.unh.edu/sites/cola.unh.edu/files/student-journals/Comm-entary2010_0.pdf [https://perma.cc/36DJ-YBUN] ("Societal norms have inevitably adapted to this new medium of communication and the level of surveillance that has come with it. "). *See generally* ROBERT ELLIS SMITH, BEN FRANKLIN'S WEB SITE: PRIVACY AND CURIOSITY FROM PLYMOUTH ROCK TO THE INTERNET (2000) (examining the changing conceptions of privacy throughout American history).

[135] *See, e.g.*, Ryan Calo, *Code, Nudge, or Notice*, 99 IOWA L. REV. 773, 788 (2014) ("Consumer preferences are also deeply heterogeneous. Some consumers wish for more privacy while others could not care less."); Daniel J. Gilman & James C. Cooper, *There Is a Time to Keep Silent and a Time to Speak, the Hard Part Is Knowing Which Is Which: Striking the Balance Between Privacy Protection and the Flow of Health Care Information*, 16 MICH. TELECOMM. & TECH. L. REV. 279, 318 (2010) (discussing the heterogeneity of privacy preferences in the context of health-related data); Pamela Samuelson, *Privacy as Intellectual Property?*, 52 STAN. L. REV. 1125, 1134–35 (2000) ("Although some individuals may value privacy so highly that they will choose not to engage in market transactions about their personal data, others may be quite willing to sell their personal data to firms *A*, *B*, and *C* (even if not to *X*, *Y*, or *Z*)."); Lior Jacob Strahilevitz, *Toward a Positive Theory of Privacy Law*, 126 HARV. L. REV. 2010, 2026 (2013) ("American attitudes toward privacy are highly heterogeneous . . . ."); Kay Connelly et al., Do I Do What I Say?: Observed Versus Stated Privacy Preferences 623 (2007) (unpublished manuscript), https://link.springer.com/content/pdf/10.1007/978-3-540-74796-3_61.pdf [https://perma.cc/N8L6-FERM] (measuring privacy concerns in various computing environments).

today), and halt the development of novel business models.[136] The task is thus to induce not a static, maximal privacy protection, but a dynamic standard that would mirror diverse expectations and evolve with time and with social norms.[137]

In light of these assumptions, I propose that the criteria for the rating would not be "objective" nor set by regulation. Nor should the model reward the most privacy-protective measures. This article is agnostic as to the "right" level of privacy users "need," and is rather concerned more humbly with ensuring that users' views of their privacy interests would be taken into account.[138] Thus, the rating should strive to reflect *users' own* views of their privacy interests, as they change over time.

Specifically, I propose to establish a dynamic privacy rating for social networking firms. The rating would measure two factors: the first is users' *expectations*, namely, are users *surprised* when they find out about data practices of their social networks. The second is users' *satisfaction*—are users *concerned* about their social network's data practices. "Surprises" and "concerns" would be represented in the model as a penalty in the privacy grade of the platform, to which the executive compensation would later be linked.

How would "surprises" and "concerns" be calculated? In general terms, the task of the rating process is twofold. First, to identify privacy practices that firms engage in—such as using location services, keeping data perpetually, and using cookies and other mechanisms to collect data when the product is not in use.[139] Second, to find out whether users are (1) aware of these practices, and (2) approve of these practices.

Learning about firms' privacy practices is relatively easy. These practices are usually public knowledge or inferable from privacy policies. It is also possible to use technology to reveal some privacy practices of social media companies. For example, it is possible to inspect when a service tracks users' location, and

---

[136] *See* Strahilevitz, *supra* note 135, at 2039–40 ("[R]eal-world costs associated with enhanced privacy" include, for example, "statistical discrimination on the basis of observable characteristics, anticompetitive behavior, or the imposition of elite preferences on a populist populace."). *But see* Julie E. Cohen, *What Privacy Is For*, 126 HARV. L. REV. 1904, 1918–27 (2013) (arguing that *lack* of privacy may harm innovation).

[137] *Cf.* Felix T. Wu, *The Constitutionality of Consumer Privacy Regulation*, 2013 U. CHI. LEGAL. F. 69, 75 (2013) (fostering notice-and-choice "because it avoids a one-size-fits-all approach to privacy and potentially opens the space for companies to serve consumers' heterogeneous privacy preferences differently").

[138] Social networks that operate in the global scale may be under obligation to apply other jurisdictions' laws as well, such as GDPR. *See supra* note 40.

[139] *See, e.g.*, sources cited *supra* note 53.

whether it uses cookies to track users on other websites.[140] Technologies can also examine the data protection methods firms use.[141] Such tools can be deployed involuntarily on any website and can help gather data about privacy practices of social networks.

Next, the rating process would need to seek users' feedback about the networks' practices in order to calculate "surprises" and "concerns."[142] The best way to achieve this would be to require social networks to survey users about their privacy practices.[143] One option to conduct a survey is to collect users' perceptions through crowdsourcing platforms such as Amazon Mechanical Turk.[144] A better option is to reach users via each social media directly, and factor the response rate into the rating, in order to induce social media firms to encourage their users to respond. It is also possible to reward firms that have a high response rate and to penalize firms with a low response rate.

Surveys could be complemented by other data. For example, it is possible to measure the number of times a site's privacy policy has been accessed (the more it was accessed, the lower the "surprise" factor), and the transparency level of Privacy Policies.[145] A recent project by Joel Reidenberg, Jaspreet Bhatia, and Travis D. Breaux proposes a semantic analysis of Privacy Policies' ambiguity, which yields a transparency score for Privacy Policy documents.[146] This score can be factored into the "surprise" grade of the firm.

---

[140] *See, e.g.*, COOKIE CHECKER, http://www.cookie-checker.com/ [https://perma.cc/2VCP-RXTY].

[141] It may be possible to incorporate rating services that already exist on the market into the rating. *See, e.g.*, SECURITY SCORECARD, https://securityscorecard.com/ [https://perma.cc/J9KR-EU94].

[142] Importantly, the surveys should also capture users' perception with regard to the purpose of the practice, because the purpose of collecting data may be material to users' perception of it. For example, users may feel comfortable if the network collects location data in order to deliver location-based services, yet frown upon the collection of the same data for advertising purposes. *See* Lin et al., *supra* note 56, at 199 ("[A] user's willingness to grant a given permission to a given mobile app [to use their data] is strongly influenced by the purpose associated with such a permission.").

[143] Firms may try to manipulate the results by only nudging privacy-indifferent users to participate in the survey (social networks are likely to know their users' attitudes towards privacy). Yet this concern is attenuated because privacy-aware users would need to be nudged less. In any event, sample bias—i.e., the concern that some members of the intended populations are more likely to be included in the survey than others—must be taken into account if surveys are conducted. *See, e.g.*, Ann Bowling, *Mode of Questionnaire Administration Can Have Serious Effects on Data Quality*, 27 J. PUB. HEALTH 281, 284 (2005) (discussing sample bias).

[144] *See* AMAZON MECHANICAL TURK, https://www.mturk.com/ [https://perma.cc/RF42-3PPY].

[145] Of course, such a move can also incentivize firms to attract users to their Privacy Policy.

[146] Joel R. Reidenberg et al., *Ambiguity in Privacy Policies and the Impact of Regulation*, 45 J. LEGAL STUDIES S163, S176–77 (2016).

What privacy practices of social networks should the rating examine? The starting point is that the privacy rating must be dynamic and examine privacy issues that are relevant to users, as they change over time. Indeed, the rating criteria would need to be updated periodically as new privacy challenges emerge.[147] For example, in this day and age it would be important to examine use of location services and cookies, among other things. In a year's time, other issues may become more important, perhaps moving users' information to a blockchain, or connecting users' information with information derived from wearable technology.[148]

How would the rating be calculated? To calculate the score, a rating agency can average the scores for each factor across all the networks and use the average score as a baseline. "Surprises" and "concerns" should have an equal weight in the final privacy grade. Firms would be ranked based on this average to determine their privacy score. Firms that would be ranked above the average would be able to give a *bonus* to their executives. Firms that would rank below the average would need to give a *penalty* to their executives in their compensation scheme.

Indeed, this mechanism would compare companies to each other and not to any objective standard. The rationale to use this comparative mechanism is twofold. First, the comparative ranking is likely to better generate a vital privacy competition. Second, I believe that social networks can offer low privacy protection and be ranked low in this regard—but still have the right to exist, if users know of this feature in advance and can plan, for example, what information to share on such platforms.

2. Governance and Facilitation

The second challenge to address is how to govern and facilitate the rating system. A main question in this regard is under what umbrella the rating agency should be operating and how it should be funded. One option is to allocate this task to private rating companies. This option would resemble existing

---

[147] There are of course issues related to surveys, such as self-selection bias, question phrasing challenges, social desirability effects, etc. *See, e.g.*, Bowling, *supra* note 143, at 283–88 (discussing non-measurement and measurement error that relate to surveys). Yet there is no reason to believe the same issues would not affect all social networks equally. It would thus be possible to factor for them when analyzing the results if they prove to be substantial or to normalize the result. In any case, the survey results would still provide a substantial improvement over the current regime, where users' input is not being sought at all.

[148] The SEC updates the criteria for incentive-based schemes in other contexts as well. *See, e.g.*, Pay Versus Performance, 80 Fed. Reg. 26,330 (proposed May 7, 2015).

rating mechanisms in other industries, such as corporate governance rating agencies[149] or the American hotel industry rating system.[150] Under such models, private, independent rating bodies issue ratings of players in certain industries based on criteria they set and charge the companies that they rank.

Applying this model in the social media privacy context would mean establishing a rating agency for social network privacy. The rating agency would design the criteria for the privacy score, collect the data they need, and facilitate and calculate the rating. The agency would likely be funded by fees it would collect from the rated social networks themselves.[151]

It is possible to create more than one rating agency in order to encourage competition between the rating agencies and curb the costs they would charge firms for the ranking. There is, however, a risk that besides price competition, multiple rating agencies would create a race to the bottom in terms of privacy standards. Therefore, more than one rating company would only be desired if the rating companies would not be setting the rating criteria, an option discussed below.

Another option is to implement the model under the auspices of the FTC.[152] In this option, the FTC would set the criteria, examine social networking companies' conduct, and issue the ranking. A main advantage of this option over the option of private rating agencies is compliance, because the FTC's leadership in the privacy area is well established and its guidelines and instructions are typically well observed.[153] Managing the system at the FTC would also produce information advantages, as the FTC would gain first-hand and up to date information about firms' practices and users' privacy

---

[149] Corporate governance rating agencies are companies, such as Institutional Shareholders Service (ISS), that rate corporate governance. *See, e.g.*, INSTITUTIONAL SHAREHOLDERS SERV., https://www.issgovernance.com/ [https://perma.cc/DS2K-JVPJ]. The rating is used mainly by institutional investors in the investment decision-making process.

[150] In the United States, independent rating companies issue the one-to-five stars rating for hotels and restaurants. *See, e.g*, *About*, FORBES TRAVEL GUIDE https://www.forbestravelguide.com/about [https://perma.cc/94RZ-4N3S] (follow "Learn How We Inspect"); AAA Travel Guides, AAA https://www.aaa.com/travelguides/ [https://perma.cc/4WDF-SWBU]. In other countries, the one-to-five star hotel rating system is being facilitated by governments (France), or by volunteer bodies (Germany). *See New Hotel Rating System*, ATOUT FRANCE, https://uk.france.fr/en/holiday-prep/new-hotel-rating-system [https://perma.cc/3639-Y7F8]; *Criteria Hotelstars Union: Excerpt of the Catalogue of Criteria*, HOTELSTARS.EU, https://www.hotelstars.eu/criteria/ [https://perma.cc/66LU-VTWQ].

[151] *See infra* Section III.B.3 for a discussion of voluntary vs. mandatory participation.

[152] *See, e.g.*, Aaron Perzanowski & Chris Jay Hoofnagle, *What We Buy When We Buy Now*, 165 U. PA. L. REV. 315, 362–65 (2017) (arguing that the FTC is a good fit to intervene in areas that involve consumer disclosures).

[153] *See* Bamberger & Mulligan, *Privacy on the Books*, *supra* note 20, at 252, 273–74 (discussing "the rise of the Federal Trade Commission's (FTC's) role as an 'activist privacy regulator' advancing an evolving consumer-oriented understanding of privacy").

interests, which can be used for formulating privacy standards and policies in other contexts as well.[154]

On the other hand, managing such a task within a regulatory body potentially has substantial drawbacks. A key concern touches on capture and public choice problems.[155] Specifically, the FTC may be influenced by industry players, whose interests (to receive a good rating without changing much of their operation) would affect the way the agency sets the criteria and calculates the scores. Capture can have both privacy and competitive effects, because not only would incumbents push for lax standards for data use, but they are also likely to promote standards that would favor them compared to new entrants, who may lack the political power and capital needed to influence the agency.[156]

After weighing the advantages and disadvantages of private and public mechanisms, the best way to promote the idea is to create a hybrid private-public model. Under a hybrid framework, the FTC would be responsible for setting the privacy criteria to be examined and to supervise the deployment of the model. The private agencies would be tasked with gathering the data, calculating the score, and publicizing the ranking. This way, the FTC review of the rating process is built in to the system, and there is also a structural distinction between the standard-setting function and the rating function, as each is done by a separate entity.

The final step with regard to the facilitation of the model is to define how social networks themselves would implement the ranking. Indeed, after the rating company issues the scores, organs within each firm would need to incorporate the score into the firm's executive compensation scheme. This process should be managed by chief privacy officers (CPOs) or an equivalent role.[157] CPOs would need to decide which executives in the firms should be subject to this model and have their compensation

---

[154] The decision between these options may perhaps depend on whether our entire model is voluntary or not. *See infra* Section III.B.3.

[155] *See* Richard Pierce, *Institutional Aspects of Tort Reform*, 73 CALIF. L. REV. 917, 935 n.104 (1985) ("'Capture' refers to the tendency of some agencies to favor the industry they are required to regulate by protecting the industry from outside competition and stifling innovation that threatens the status quo in the industry." (citing Noll, *The Behavior of Regulatory Agencies*, 9 REV. SOC. ECON. 15 (1971)); Thomas W. Merrill, *Capture Theory and the Courts: 1967–1983*, 72 CHI.-KENT L. REV. 1039, 1050 (1997) ("[A]gencies were likely to become 'captured' by the business organizations that they are charged with regulating.").

[156] Examples for such standards may include an excessive focus on data storage or data management procedures that in fact are relevant mainly for large players.

[157] *See* Bamberger & Mulligan, *Privacy on the Books*, *supra* note 20, at 261–62 (discussing the position of CPOs).

affected by the firm's privacy score. In general, because of the centrality of privacy decisions in social networking firms on the product, financial, and policy levels, virtually all executives have a role in defining the contours of privacy allocated to the firms' users.[158] Thus, absent special considerations, I assume that all executives in the firms would be subject to this proposal.[159] The compensation committee of the firm would then be tasked with designing a formula to factor the ranking into the executive compensation. To prevent manipulation, I propose to include the executive committee's work process in the list of items that the annual external audit is required to examine.[160]

3. Adoption and Enforcement of the Model

The final challenge is to compel social networking firms to adopt the model and adequately factor the ranking into their executive compensation package. There are two options in this regard. The first is to design the model as an optional, voluntary framework and hope for social networks to opt in and adopt it voluntarily. The second option is to impose this model by a regulatory order (such as an FTC instruction), or to include it in the FTC's "best practices," which are voluntary *de jure* but nearly compulsory *de facto*.[161]

The voluntary option only resonates if a critical mass of social networking firms is believed to opt in, because only a large-scale adoption of the model can reverse the current rush to

---

[158] The notion of Privacy by Design, for example, means that firms need to consider data protection when designing information technologies and systems. *See* Ira S. Rubinstein, *Regulating Privacy by Design*, 26 BERKELEY TECH. L. J. 1409, 1411-12 (2011) (describing privacy by design as "a systematic approach to designing any technology that embeds privacy into the underlying specifications or architecture."). The "Privacy by Design" term was coined by the Information and Privacy Commissioner of Ontario, Canada. *See* ANN CAVOUKIAN, PRIVACY BY DESIGN: THE 7 FOUNDATIONAL PRINCIPLES (Aug. 2009), https://www.ipc.on.ca/wp-content/uploads/resources/7 foundationalprinciples.pdf [https://perma.cc/VHY6-VAJV]; *see also* FTC 2010 REPORT, *supra* note 66, at 39–78 (proposing new frameworks to protect consumer data, in part in lieu of the 'privacy by design' principles); Stuart L. Pardau & Blake Edwards, *The FTC, the Unfairness Doctrine, and Privacy by Design: New Legal Frontiers in Cybersecurity*, 12 J. BUS. & TECH. L. 227, 264 (2017) (noting that Ann Cavoukian "introduced the 'foundational principles' of [privacy by design] in the mid-1990s.").

[159] For example, the business departments of the firm are responsible for what data is being sold and for what price; the technological and engineering unit of the company is responsible for the system design, including the embedded data practices and the default privacy settings. *See* sources cited *supra* note 158 (discussing the privacy by design concept).

[160] *See* discussion *infra* Section IV.A.

[161] Bamberger & Mulligan, *Privacy on the Books*, *supra* note 20, at 273–74 (discussing the influence of the FTC on decision-making within firms) (internal quotation marks omitted).

the bottom trend in privacy protection and to inject privacy competition into the system.

Are firms likely to adopt this model voluntarily?[162] On the one hand, as discussed, an enhanced privacy standard is consistent with the firm's long term shareholders' interests.[163] If managers pursue less protection than shareholders would have wanted, it should be possible to convince shareholders to adopt the proposal via a shareholders' resolution or a "say on pay" vote.[164] To "nudge" firms in this direction, if needed, the U.S. Securities and Exchange Commission (SEC) can mandate an annual shareholder vote on whether the company ought to consider opting in to linking executive pay to privacy ratings.[165]

On the other hand, there is a gap between the privacy standard needed to align the interests of executives—the long-term interest of the company—and the privacy standard desired from a societal point of view, which the model aims at. Shareholders are far less likely to opt in to a higher privacy standard that is aimed at curing externalities that the firm imposes on others (and that shareholders in fact benefit from, at least in the short term).[166] The firm may have *some* incentive to opt in in this case, for reputational considerations and signaling effect (signaling superiority to the users on privacy matters). And shareholders will have some more incentive to curb such conduct because of its long-term harm. Yet, these are limited incentives which are not likely to sufficiently push the needle.[167]

---

[162] A question may arise as to why shareholders have not adopted such an idea themselves. The reason may involve the rush to the bottom dynamics with regard to privacy protection, as Part I discusses, and the well-known overrepresentation of managers' interests and positions in firms' decision-making. *See, e.g.*, BEBCHUK & FRIED, *supra* note 12, at 23–44 (discussing the management influence on compensation and other issues).

[163] *See* discussion *supra* Section II.A.

[164] "Say-on-pay" is a nonbinding vote on executives' compensation packages and is a prevalent tool to control executive pay. *See* Jeffrey N. Gordon, *"Say on Pay": Cautionary Notes on the U.K. Experience and the Case for Shareholder Opt-In*, 46 HARV. J. ON LEGIS. 323, 339–40 (2009) (describing shareholder efforts to advance say-on-pay proposals); Andrew C. W. Lund, *Say on Pay's Bundling Problems*, 99 KY. L.J. 119, 122 (2010) (noting that several corporations have voluntarily adopted say-on-pay, often at shareholders' active push); *see also 2009 Proxy Season Scorecard*, RISKMETRICS GROUP (Dec. 15, 2009), http://www.shareholderforum.com/sop/Library/20091215_RiskMetrics-Scorecard.pdf [https://perma.cc/6W5R-AFN5] (noting that "say-on-pay" was the most prevalent shareholder proposal submitted in 2009).

[165] Several federal bills have incorporated say-on-pay proposals, though none of them was implemented so far. *See, e.g.*, Shareholder Bill of Rights Act of 2009, S. 1074, 111th Cong. (2009); Shareholder Empowerment Act of 2009, H.R. 2861, 111th Cong. (2009); Shareholder Vote on Executive Compensation Act, H.R. 1257, 110th Cong. (2007); Shareholder Vote on Executive Compensation Act, S. 1181, 110th Cong. (2007).

[166] *See* Jesse M. Fried, *The Uneasy Case for Favoring Long-Term Shareholders*, 124 YALE L.J. 1554, 1621 (2015) ("Neither short-term nor long-term shareholder interests can be counted on to align with the interests of non-shareholder parties.").

[167] *See supra* Part I.

In the real world, proposals to tie executive compensation to goals that do not directly promote shareholders' interests have usually proved futile. In the 1990s, proposed resolutions to tie executive pay to the firm's social performance, such as environmental effects, proliferated, but never passed.[168] Proxy advisory service Glass Lewis has fruitlessly recommended linking short-term incentives to "employee turnover, safety [records], environmental issues, and customer satisfaction."[169] In Australia, the ASX Corporate Governance Council has proposed to link executive compensation to diversity objectives.[170] Shareholders' support for these proposals has been consistently low.[171] Granted, there is more direct benefit for shareholders from my proposal than from those other examples, because the disregard for privacy may very well harm firms in the long run.[172] Yet, at the end of the day, shareholders are still unlikely to opt in if the privacy standard reflects societal interests and not their own.

In case firms would not opt in voluntarily, a regulatory mandate would be a more promising way forward. The most straightforward way to achieve that is via a ruling by the FTC that social networks must participate in the rating process and incorporate its results into their executive compensation schemes.[173] Alternatively, it would probably be sufficient to include this model as part of the FTC Best Practices, which are usually hastily adopted as the industry standard. Under either these "hard law" or "soft law" mechanisms, all social networking firms would be involuntarily rated, and companies would be compelled to tie part of the executive compensation to that privacy rating.[174]

---

168 *See* Lori B. Marino, Comment, *Executive Compensation and the Misplaced Emphasis on Increasing Shareholder Access to the Proxy*, 147 U. PA. L. REV. 1205, 1215–16, 1216 n.69 (1999) (noting that proposals linking executive pay to social performance "were the most voted on type of proposal in 1997," but "received the lowest average support [7%] of any type of proposal.").

169 *See* GLASS LEWIS & CO., PROXY PAPER GUIDELINES, 2014 PROXY SEASON: AN OVERVIEW OF THE GLASS LEWIS APPROACH TO PROXY ADVICE 21 (2014), http://www.glasslewis.com/assets/uploads/2013/12/2014_GUIDELINES_Canada2.pdf [https://perma.cc/VV29-PT5Y].

170 *See* ASX CORPORATE GOVERNANCE COUNCIL, CORPORATE GOVERNANCE PRINCIPLES AND RECOMMENDATIONS 11 (3d ed., 2014), http://www.asx.com.au/documents/asx-compliance/cgc-principles-and-recommendations-3rd-edn.pdf [https://perma.cc/F97K-KXNB].

171 *See* Marino, *supra* note 168, at 1215–16.

172 *See* discussion *supra* Section II.A.

173 As discussed in Part I, legally speaking, the FTC can be assigned this task under Section 5, pursuant to their authority to regulate unfair or deceptive practices in or affecting commerce. As discussed, this authorization that has so far been interpreted quite broadly. *See supra* note 11 and accompanying text.

174 *See* discussion *supra* Section II.B.2.

C. The Benefits of the Model

The Pay for Privacy model would boost the overall value creation of social media. It would motivate an efficient level of privacy protection in the industry and enhance users' trust in social media platforms. In turn, users' trust would encourage vibrant use of social media for the benefit of users, social networks, shareholders, and society as a whole. At the same time, this model would retain the flexibility to develop novel business models in the social media industry—*including* ones that exploit users' personal data—as long as privacy interests are internalized. An additional salutary effect of the model is informational: prevalent data practices in social media firms, as well as users' perceptions of such practices, would come to light. This information could encourage privacy competition in the industry, and guide decision-makers in other industries.

First and foremost, the model would create a powerful incentive for social network executives to internalize users' interests ex ante, because failing to do so would adversely impact their compensation ex post. Indeed, factoring users' interests into executive compensation schemes would counter the incentive to trade users' data whenever doing so would maximize short term revenues.[175] Notably, a key part of the model is that no external force would be dictating the desired privacy levels. Rather, the system would be geared towards revealing and satisfying the privacy standards users themselves are expecting.[176]

By heeding users' privacy concerns, the model would boost users' trust, and encourage the use of social media in the long term. Continued use of social media is socially desirable. Users are the first group of beneficiaries of social networks. Social networks provide them with a platform to post and consume content, and to interact with each other.[177] But users' engagement on social networks also produces spillovers on society as a whole. Social networking fosters speech and creativity, facilitates inter-personal connections, and generates opportunities for cooperation and prosperity irrespective of physical or geographical limitations. Finally, social media companies and their shareholders would evidently profit from a

---

[175] *See* discussion *supra* Section II.B.1.

[176] Because users are a diverse group with diverse privacy expectations, it would be possible that different social networks would offer different privacy expectations, and they would all be acceptable to their users. *See* Calo, *supra* note 135, at 788 ("Consumer preferences are also deeply heterogeneous. Some consumers wish for more privacy while others could not care less.").

[177] boyd & Ellison, *supra* note 3; *see also supra* note 1 (discussing the time individuals invest in social media, which is an indication of the utility it produces for them).

high volume of users and activity on social media. This proposal would align the interests of executives with all these groups of beneficiaries, to ensure that users' privacy concerns would not jeopardize those benefits.

Another advantage of my model is informational. First, the model would create, as a byproduct, a transparent privacy rating of social networks and expose their privacy practices. The privacy rating of social networking firms would allow users to understand firms' privacy offerings without tediously reviewing complex privacy settings.[178] The ability to meaningfully compare firms on privacy terms could counter the race to the bottom dynamics previously discussed and inject privacy competition into the market.[179] Moreover, for the first time, executives would have an incentive to improve privacy disclosure rather than to keep the matter dormant, because informed users would boost the "surprises" score. Likewise, firms and their executives would have an incentive to learn about users' privacy preferences, in order to avoid *surprises* and *concerns,* which would harm their privacy score.[180]

Most importantly, this model would achieve all the above benefits without curtailing the marketability of personal data.[181] Data-based business models are not bad *per se*. Knowledge about users can boost efficiency in the retail industry, by preventing waste in marketing spending and by tailoring products and services better to users' needs.[182] The model would not prevent firms from exploring new uses of data. Executives would only be penalized if these new uses are unacceptable to their users, even if market failures prevent them from voting on it with their feet.[183]

Finally, privacy poses a critical threat to other internet businesses and entities, many of which may also benefit from my proposal. First, improved privacy standards on social media are likely to create spillovers to other industries. By providing a low-cost method to communicate user privacy expectations to the market, more companies are likely to listen to users' preferences. Consider also that leading social media firms constantly

---

[178] *See supra* note 44 and accompanying text.

[179] *See supra* notes 96, 99–100 and accompanying text.

[180] *See supra* note 137 and accompanying text.

[181] FED. TRADE COMM'N, BIG DATA: A TOOL FOR INCLUSION OR EXCLUSION? at i (2016), https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf [https://perma.cc/RB9N-R3DT] ("[Data] can guide the development of new products and services, predict the preferences of individuals, help tailor services and opportunities, and guide individualized marketing.").

[182] *Id.*

[183] *See supra* Part I (discussing market failures users are subject to when attempting to make privacy-related decisions).

penetrate additional markets and put out various types of products and services.[184] It is likely that their privacy practices in the social media space would inform their behavior and policies in the other new activities. Second, the Fourth Amendment ties the applicable legal standard of privacy to "reasonable expectations of privacy," and so the more users would learn to expect better privacy terms from online companies the more privacy they would be entitled to.[185] Third, the model can inform regulatory and enforcement strategies moving forward in a variety of domains, such as mobile apps, search engines, and other data-centric digital services.

III. OBJECTIONS

Three main critiques can be raised against the proposed model. The first is that the model can be easily manipulated by firms and executives, and that these manipulations would thwart its advantages. The second is that this model targets an imagined problem, because privacy is not an interest the law needs to protect—in particular in the social networking realm. The third possible concern is that it is possible to tie executive compensation to various interests and values, and that the focus on privacy is unjustified compared to others. Below I analyze and respond to these arguments.

A. Manipulations of the Model

One challenge that the model faces is that firms and executives may manipulate the model in order to receive bonuses despite actually maintaining low privacy protection.[186] Executives would be able to tamper with the reports used to formulate their firm's privacy score, report users' responses

---

[184] For example, Facebook is expanding into the realms of Artificial Intelligence, virtual reality, and connectivity. *See, e.g.*, Jessica Conditt, *Facebook's Plans for Oculus Are Finally Taking Shape*, ENGADGET (Apr. 19, 2017), https://www.engadget.com/2017/04/19/facebooks-plans-for-oculus-are-finally-taking-shape/ [https://perma.cc/NS2A-8RKH] (discussing Facebook's acquisition of Oculus); Mike Elgan, *The Surprising Truth About Facebook's Internet.org*, COMPUTERWORLD (Feb. 15, 2016, 3:15 AM PT), http://www.computerworld.com/article/3032646/internet/the-surprising-truth-about-facebooks-internetorg.html [https://perma.cc/27AZ-HDC9] (discussing Facebook's infrastructure venture Internet.org).

[185] *See* Ohm, *supra* note 45, at 927 (discussing arguments that were raised in legal proceedings regarding the lack of "reasonable expectations of privacy" in different settings (internal quotations omitted)).

[186] *See* Bebchuk et al., *supra* note 105, at 754 ("[C]ompensation arrangements approved by boards often deviate from optimal contracting because directors are captured or subject to influence by management, sympathetic to management, or simply ineffectual in overseeing compensation.").

selectively, refer the surveys only to users who they identify as privacy indifferent, or ask survey questions in a way that encourages favorable answers.[187] Indeed, especially after the backdating accounting crisis, executives are not perceived trustworthy in reporting parameters that affect their pay.[188] What is more, the compensation committee of the firm can design a formula to compensate executives for a pay penalty that originates from a low privacy score by boosting other parameters that will increase the bottom line for the executives.[189]

It is important to note that manipulation of Pay for Performance schemes are a well-known challenge in corporate governance, and are in no way specific to this model.[190] For example, 'correction measures' to compensate executives for lost bonuses were observed after the Dodd-Frank act enacted a "say-on-pay" mechanism, which required companies to hold a vote on executive compensation at least once every three years.[191] The result was that even when companies reduced some aspects of pay in anticipation of the say-on-pay vote, they offset this by

---

[187] *See supra* note 143.

[188] *See* Natasha Burns & Simi Kedia, *The Impact of Performance-Based Compensation on Misreporting*, 79 J. FIN. ECON. 35, 37 (2006) (finding empirically a correlation between the link of CEO's option portfolio to stock price and the likelihood to misreporting). *See generally* David Aboody & Ron Kasznik, *CEO Stock Option Awards and the Timing of Corporate Voluntary Disclosures*, 29 J. ACCT. & ECON. 73 (2000) (showing that executives manage the timing of voluntary disclosures to manipulate the stock value—and their options—favorably); John C. Coffee, Jr., *A Theory of Corporate Scandals: Why the USA and Europe Differ*, 21 OXFORD REV. ECON. POL'Y 198, 202 (2005) (showing that executive compensation has a key role in securities fraud); Jared Harris & Philip Bromiley, *Incentives to Cheat: The Influence of Executive Compensation and Firm Performance on Financial Misrepresentation*, 18 ORG. SCIENCE 350 (2007) (analyzing manipulation problems that result from performance-based executive compensation schemes); David Yermack, *Good Timing: CEO Stock Option Awards and Company News Announcements*, 52 J. FIN. 449 (1997) (also showing that executives coordinate the timing of disclosures to favorably manipulate stock value and options) .

[189] *See* BEBCHUK & FRIED, *supra* note 12, at 67 (discussing how managers' compensation can be manipulated to augment managers' rents while appearing performance-based and thus more defensible); Michael S. Weisbach, *Optimal Executive Compensation Versus Managerial Power: A Review of Lucian Bebchuk and Jesse Fried's Pay Without Performance: The Unfulfilled Promise of Executive Compensation*, 45 J. ECON. LIT. 419, 425–26 (2007) (showing how firms can disguise benefits to executives in various ways to make compensation appear more performance-based than it actually is); *see also* M.P. Narayanan & H. Nejat Seyhun, *The Dating Game: Do Managers Designate Grant Dates to Increase Their Compensation?*, 21 REV. FIN. STUD. 1907 (2008) (illustrating how firms artificially raise executives' option value by various practices of option backdating and option repricing).

[190] *See, e.g.*, Bank & Georgiev, *supra* note 105, at 16 (arguing that even after the Dodd-Frank Act, Pay for Performance schemes are "ineffectual, counterproductive, and easy to manipulate").

[191] *See* Dodd-Frank Wall Street Reform and Consumer Protection Act, Pub. L. No. 111-203, § 951, 124 Stat. 1376, 1899 (2010) (codified as amended at 15 U.S.C. § 78n–1 (2012)) (setting out the say-on-pay requirement); Shareholder Approval of Executive Compensation and Golden Parachute Compensation, 76 Fed. Reg. 6010, 6011 (Feb. 2, 2011) (codified at 17 C.F.R. § 240.14a–21 (2018)) (establishing the say-on-pay regime).

increasing other components of the compensation package with the net effect of increased overall pay.[192] This model does not fare worse than the typical Pay for Performance scheme with regard to manipulation. In fact, this model may have better ways to address the challenge.

One way to address possible manipulations is already built into the model. As discussed above, my proposal is to rely as much as possible on technological and other external factors to figure out firms' privacy practices and to determine firms' privacy scores, rather than to rely exclusively on the firm's reporting.[193] As discussed, at this time, technology may not (or not yet) be at a stage to provide all the information needed for formulating the score. Reliance on the firms' reporting may still be necessary. Yet in the long run, I believe that technology can serve as an effective safeguard against certain manipulations and misapplications of the model, such as selective surveying and inadequate reporting of privacy practices. Such tasks can be easily tracked or even entirely performed with no human involvement.

Another reason that Pay for Privacy Performance is less prone to manipulation is that it is enforceable by more than one agency. Specifically, misreporting and other deceptive acts clearly fall under the FTC jurisdiction, and the agency can impose sanctions on firms that engage in such practices.[194] This regulatory measure does not only protect users ex post, but also creates an ex ante incentive for firms and executives to play by the rules.

In addition to the FTC, the SEC can serve as another enforcement wing, at least with regard to public social network firms. I propose to include the executive committee's work process in the list of items that the external audit is required to examine.[195] Thus, the firm's auditor would need to confirm that the firm adequately factored the privacy score into the annual executive pay. This mechanism would achieve two goals. First, it would compel executives and the compensation committee to execute the model adequately. Second, it would allow the SEC to

---

[192] Mathias Kronlund & Shastri Sandy, *Does Shareholder Scrutiny Affect Executive Compensation?* 4–5 (Dec. 5, 2018) (unpublished manuscript), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2358696 [https://perma.cc/A82R-9464].

[193] *See* discussion *supra* Section II.B.2.

[194] *See* Press Release, Fed. Trade Comm'n, Facebook Settles FTC Charges That It Deceived Consumers by Failing to Keep Privacy Promises (Nov. 29, 2011), http://ftc.gov/opa/2011/11/privacysettlement.shtm [https://perma.cc/6MAE-2XHM].

[195] *See* SEC. EXCH. COMM'N, PUB. CO. ACCOUNTING OVERSIGHT BD., rule 1001(a)(vii) at 23, (defining the roles of the auditor), effective pursuant to Order Approving Proposed Rules Relating to Registration System, Exchange Release No. 34-50,331, Fed. Sec. L. Rep. (CCH) § 87,256 (Sept. 8, 2004).

supervise the implementation of the proposed model in the case of public firms as part of other reports the firm submits.[196]

It is also worth pointing out that even if not all manipulations are prevented, the model would still provide a substantial improvement over the current regime. Firms and executives would still need to check the effects of their actions on privacy levels and the approval level of users to these measures, and to justify their actions in a terminology of privacy protection. This progress bears tremendous importance. Compelling firms and executives to discern users' privacy interests would change the discourse of user privacy. Firms and executives would need to articulate and defend their practices on the scope of privacy, rather than pronouncing the whole question as irrelevant and proclaiming that "privacy is dead."[197] This profound change in discourse is bound to bring along a change in practice as well.[198]

B. Imaginary Privacy Problem

A second criticism my proposal may face is that it is not aimed at a "real" issue the law needs to tackle. An extreme version of this critique concerns the lack of a right to privacy in the first place. Assertions that people with nothing to hide need not be concerned by the lack of privacy, or that privacy is nothing but a decaying social norm, abound.[199] Even those who value privacy can be skeptical regarding the focus of the model on social media companies. After all, social media companies are private, rather than governmental actors,[200] they perform data

---

[196] *See* Press Release, Sec. Exch. Comm'n, SEC Proposes Rules to Require Companies to Disclose the Relationship Between Executive Pay and a Company's Financial Performance (Apr. 29, 2015), http://www.sec.gov/news/pressrelease/2015-78.html [https://perma.cc/C4CK-4V2H].

[197] The saying that "Privacy is dead" is attributed to Mark Zuckerberg, who claimed that privacy is no longer a "social norm." *See, e.g.*, Chi Ling Chan, *Privacy Is (Not) Dead*, STAN. DAILY (Oct. 7, 2014), https://www.stanforddaily.com/2014/10/07/privacy-is-not-dead/ [https://perma.cc/VU6G-GL92]; *see also* Bobbie Johnson, *Privacy No Longer a Social Norm, Says Facebook Founder*, GUARDIAN (Jan. 10, 2010), http://www.theguardian.com/technology/2010/jan/11/facebook-privacy [https://perma.cc/HKQ3-3M4M].

[198] *See* Matthew Sag, *Internet Safe Harbors and the Transformation of Copyright Law*, 93 NOTRE DAME L. REV. 499, 534 (2017) (arguing that the Ninth Circuit's decision in *Lenz v. Universal Music Corp.* "may have ramifications" for the fair use analysis, because copyright owners themselves would begin articulating their answers in Fair Use terms).

[199] Even the status of privacy as a social norm is deteriorating, as people learn not to expect privacy, in particular when they use the internet, and even more, when they use social media. *See, e.g.*, Johnson, *supra* note 197 (arguing that privacy is no longer a social norm).

[200] James Q. Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, 113 YALE L.J. 1151, 1211 (2004) ("Suspicion of the state has always stood at the

analytics mostly on information users submit voluntarily, and they anonymize the data third parties can access, so that third parties typically cannot know the identities of the users that their ads target.[201]

There is some overlap between my response to this critique and Part I analysis. In Part I, I argued that legal intervention is justified because market failures make the social media privacy space systematically biased against users.[202] Here, I complement the picture by showing that privacy has value both as an intermediate good and as a final good, namely, for its instrumental value as well as for its own sake.[203] I show that privacy harms can yield considerable welfare loss, and that such harms are compounded in the context of social networking.

As discussed previously, the costs of inadequate privacy protection range from the tangible to the intangible. Tangible privacy risks include, *inter alia*, fraud, identity theft, stalking, and harassment.[204] Such harms are severe and can have long term effects on the individuals who experience them as well as on society as a whole.[205]

Less tangible privacy risks include discrimination, unfair treatment, reputational harms, and economic harms, such as price discrimination and inferior bargaining power.[206] For example, personal data allows social networks and third parties to provide differential and discriminatory treatment to users, and vendors who possess disproportional information on customers can easily grab users' surplus.[207]

---

foundation of American privacy thinking, and American scholarly writing and court doctrine continue to take it for granted that the state is the prime enemy of our privacy.").

[201] *See supra* note 6 and accompanying text.

[202] *See supra* Part I.

[203] *See, e.g.*, DANIEL J. SOLOVE, UNDERSTANDING PRIVACY 101–06 (2008).

[204] *See, e.g.*, Lee Rainie et al., *Anonymity, Privacy, and Security Online*, PEW RES. CTR. (Sept. 5, 2013) http://www.pewinternet.org/2013/09/05/anonymity-privacy-and-security-online/ [https://perma.cc/N7WP-4XJR] (finding that "[eleven percent] of internet users have had important personal information stolen such as their Social Security Number, credit card, or bank account information").

[205] *See, e.g.*, FTC 2010 REPORT, *supra* note 66, at 20.

[206] *See supra* note 92; *see also* JEFFREY ROSEN, THE UNWANTED GAZE: THE DESTRUCTION OF PRIVACY IN AMERICA 8 (2000) ("Privacy protects us from being misdefined and judged out of context in a world of short attention spans. . . ."); David S. Ardia, *Reputation in a Networked World: Revisiting the Social Foundations of Defamation Law*, 45 HARV. C.R.-C.L. L. REV. 261, 262 (2010) (discussing the inadequacies of defamation law in an increasingly networked world); Calo, *supra* note 88, at 999 ("Firms will increasingly be able to trigger irrationality or vulnerability in consumers . . . ."); Farrell, *supra* note 33, at 252 ("[L]oss of privacy could identify a consumer as having a high willingness to pay for something, which can lead to being charged higher prices if the competitive and other conditions for price discrimination are present.").

[207] *See, e.g.*, Acquisti & Fong, *supra* note 74 (showing that employers used social media to discriminate against job candidates).

Finally, intangible harms—such as harms to dignity, freedom, and autonomy—result from the fact that sensitive information about individuals travels away from their control and may even be used against them.[208] While these types of harms may be the most elusive, they are not by any means the least significant. The idea of being potentially watched—in itself—raises levels of discomfort so high that scholars have articulated it in Orwellian, Kafkaesque, and Bentham's Big Brother theory terms.[209]

In the context of social networking, privacy costs are dramatically compounded.[210] As explained in Part I, social networks can form a frighteningly detailed profile of their users at any given moment, and they can do so without users' intentional disclosure.[211] This allows social networks to identify moments when the users are most depleted or otherwise likely to show less resistance, and exploit it for advertisers' advantage.[212] Triggering users' irrationality can also have political significance. For example, both the Obama and the Trump campaigns employed behavioral economics to target users with specific characteristics and to press the right buttons for each potential voter.[213]

---

[208] *See, e.g.*, M. Ryan Calo, *The Boundaries of Privacy Harm*, 86 IND. L.J. 1131, 1133 (2011) (describing such harm as a the "unwelcome mental states—[such as] anxiety [or] embarrassment—that accompany the belief" of an individual (or group) that he is being "watched or monitored"); Robert C. Post, *Three Concepts of Privacy*, 89 GEO. L. J. 2087, 2092 (2001) (reviewing JEFFREY ROSEN, THE UNWANTED GAZE: THE DESTRUCTION OF PRIVACY IN AMERICA (2000)) (discussing the concepts of dignity, autonomy, and knowledge); Calo, *supra* note 88, at 1029.

[209] REG WHITAKER, THE END OF PRIVACY: HOW TOTAL SURVEILLANCE IS BECOMING A REALITY 160–61 (1999) (discussing harms that result from data collectors serving as "Big Brothers"); Kate Schatz Byford, *Privacy in Cyberspace: Constructing a Model of Privacy for the Electronic Communications Environment*, 24 RUTGERS COMPUTER & TECH. L.J. 1, 50 (1998) (discussing the "Orwellian overtones" of the online space); James P. Nehf, *Recognizing the Societal Value in Information Privacy*, 78 WASH. L. REV. 1, 13 (2003) ("[Kafka's] *The Trial* captures the sense of helplessness and vulnerability we may experience when large bureaucratic organizations—or a multitude of smaller, private ones—collect information about us and possess the power to use it against our interests."); Bryan S. Schultz, Comment, *Electronic Money, Internet Commerce, and the Right to Financial Privacy: A Call for New Federal Guidelines*, 67 U. CIN. L. REV. 779, 797 (1999) ("[S]ociety inches closer to fulfilling George Orwell's startling vision of a nation where 'Big Brother' monitors the who, what, where, when, and how of every individual's life."); Daniel J. Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, 53 STAN. L. REV. 1393, 1396, 1419–23 (2001) ("Commentators have adapted the Big Brother metaphor to describe the threat to privacy . . . .").

[210] Holland, *supra* note 37, at 894 (describing privacy ramifications of social networks).

[211] *See supra* note 91 and accompanying text.

[212] *See supra* note 88 and accompanying text.

[213] Sasha Issenberg, *How Obama's Team Used Big Data to Rally Voters*, MIT TECH. REV., (Dec. 19, 2012) https://www.technologyreview.com/s/509026/how-obamas-team-used-big-data-to-rally-voters/ [https://perma.cc/H873-S7UQ]; Philip Bump, *All the Ways Trump's Campaign Was Aided by Facebook, Ranked by Importance*, WASH. POST, (Mar. 22, 2018),

Privacy costs in the social media context are further intensified because social networks' Terms of Service typically forbid anonymous use or registration under fake identities.[214] This allows the firms to reach individuals with laser-like precision, and to link information to a specific, real person. Social networks also track users online outside of the social network site and gather information about nonusers who visit their sites. What is more, consolidation in the social network market leads to mass databases of users being held by a limited number of firms.[215] Consolidation does not only jeopardize competition as discussed in Part I, but also threatens large scale information leakage.[216]

Importantly, the fact that social networks keep users' identities anonymous towards advertisers does not alleviate privacy concerns one bit.[217] Advertisers do not need to know who the user is in order to flirt with the limits of her ability to act in her best interests. Imagine an advertiser who requests Facebook to serve an ad to teens of color who feel insecure and lonely. Knowing specific identities are immaterial to that marketer's ability to turn these characteristics and weaknesses into profit. Marketers can even harass users on social media unintentionally, by targeting users for ads that may fit their profiles but at the same time harass them, as exemplified in the infamous stories of customers who continue to receive baby-related product ads after miscarriages.[218]

---

https://www.washingtonpost.com/news/politics/wp/2018/03/22/all-the-ways-trumps-campaign-was-aided-by-facebook-ranked-by-importance/ [https://perma.cc/K5HB-E62Y].

[214] *See, e.g.*, *Terms of Use*, FACEBOOK, https://www.facebook.com/terms.php [https://perma.cc/S7PS-W7E6] (requiring users to "use the same name that [they] use in everyday life" and "provide accurate information about [themselves]"); *User Agreement*, LINKEDIN, http://www.linkedin.com/legal/user-agreement [https://perma.cc/7F6G-NPTV] ("[Y]ou will . . . [p]rovide accurate information . . . [and] [u]se your real name on your profile."). Even when users can have anonymous profiles, such as on Tumblr, the firm itself can and does track a user's activity. *See, e.g.*, Privacy Policy, TUMBLR, https://www.tumblr.com/policy/en/privacy [https://perma.cc/K2H5-F8LG].

[215] On the tendency of the social networking market to centralize, see *supra* notes 100–101 and accompanying text.

[216] *See, e.g.*, Libby Watson, *Facebook 'Bug' Automatically Leaked Moderators' Identities to Suspected Terrorists*, GIZMODO (June 16, 2017), http://gizmodo.com/facebook-bug-automatically-leaked-moderators-identities-1796164403 [https://perma.cc/WJ8S-CMQ8].

[217] *See* Jane Yakowitz, *Tragedy of the Data Commons*, 25 HARV. J. L. & TECH. 1, 3–4 (2011) (asserting that the dangers of de-anonymization are overstated, and the benefits of data mining understated). *But see* Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701, 1703–04 (2010) (arguing that de-anonymizing is too routine for privacy statutes to exempt anonymized data from their ambit).

[218] *See, e.g.*, Sarah Sluis, *(Accidentally) Marketing After a Miscarriage*, CRM BLOG (Feb. 10, 2014), http://www.destinationcrmblog.com/2014/02/10/accidentally-marketing-miscarriage/ [https://perma.cc/5XTU-9LAS]. Note however that the leading social networks allow users to block unwanted content, which somewhat alleviates this concern. *See, e.g.*, Laura Entis, *Facebook Now Lets You Block the Annoying Content Your Friends Want You to Read*, ENTREPRENEUR (Mar. 5, 2014), https://www.entrepreneur.com/article/231975 [https://perma.cc/QM72-4CY6].

Notably, the privacy harms discussed have very little to do with whether an individual is in fact a 'normative person with nothing to hide' or not.[219] Despite popular thinking, big data does not represent an 'objective truth' about individuals.[220] Clearly social networks lack incentive to bother to create the most nuanced account on their users, and are likely to focus on traits that have commercial value. As a result, 'normative people with nothing to hide' (whatever this term means) are exposed to the same hazards resulting from the use of their data by social networks.[221]

To balance the picture, clearly not all uses of personal data raise these concerns. But uses that occur without taking users' interests into account are prone to precisely these concerns. The balance this Article aspires to, namely, to make executives internalize users' changing expectations is designed to allow these transactions to occur as long as interests are internalized.

C. Why Focus on Privacy?

Privacy is not by any means the only societal implication of social networks. Nor is it the only pressing societal issue. In theory, the proposal to harness executive compensation to achieve societal goals could apply to any other societal goal that firms can impact. Why then does the proposed model single out privacy?

The short answer is that the proposal is not in principle limited only to privacy protection. It is theoretically possible to link executive compensation to other societal goals in order to tilt the incentives of decision makers to promote them. I do however think that privacy provides the best test case for such a move, for multiple reasons. First, the interests of the firm and the societal interest point in the same direction—increasing privacy protection. As discussed above, even from shareholders' point of view, it is shortsighted to exploit users' data to the

---

[219] Susan Freiwald, *Online Surveillance: Remembering the Lessons of the Wiretap Act*, 56 ALA. L. REV. 9, 11 (speculating that people do not make themselves aware of the dangers of online privacy because, *inter alia*, "[w]e may consider ourselves too unimportant to be monitored, or feel confident that we have nothing to hide"); DANIEL SOLOVE, NOTHING TO HIDE: THE FALSE TRADEOFF BETWEEN PRIVACY AND SECURITY 1–3 (raising and rebutting the argument that "[i]f you've got nothing to hide, you shouldn't worry about government surveillance").

[220] *See, e.g.*, Quentin Hardy, *Why Big Data Is Not Truth*, N.Y. TIMES (June 1, 2013) https://bits.blogs.nytimes.com/2013/06/01/why-big-data-is-not-truth/ [https://perma.cc/582Q-SH8C].

[221] *See e.g.*, Sovern, *supra* note 57, at 1053 ("For example, the incontinent women who requested free samples may object to disclosure of their condition, not because they are trying to conceal criminal or immoral conduct or because they wish to exploit the ignorance of others, but because they fear humiliation if others find out." (footnotes omitted)).

fullest.[222] This makes social media privacy a fitting candidate for such a proposal.

Second, privacy went through a transformation—from being threatened mainly by governments in the past to being threatened mainly by private bodies today.[223] Still, market tools are unequipped to deal with privacy because of the market failures discussed in Part I, and regulation is unlikely to be effective because of the very dynamic nature of privacy interests. It makes sense to search for ways to incentivize the market to work in a way that is more aligned with the societal privacy interest rather than to impose a top down regulation or to accept the existing inefficiency of market operation.

Thus, this tool can be extended to other areas that bear a resemblance to the privacy issue. Such a model can be relevant in cases where externalities amount, and where the long-term interest of firms points to the same direction (though perhaps not in the same magnitude) as the societal interests, yet executives are still unmotivated to pursue these goals.

CONCLUSION

The privacy debate has generated polarizing views. On the one end of the continuum, it has been argued that privacy is an outdated concept, and that "privacy is dead."[224] On the other tip of the scale, the argument has been that the tracking of and transactions in individuals' data is *a priori* wrong. Linking executive pay to a company's privacy protection practices is a safer middle ground that allows trade in user data on the one hand but discourages abuse of this data on the other. Common executive compensation practices produce both an agency problem and an externality: they push towards less privacy protection than rationally desired by the owners of social networks and they externalize privacy costs to users and to society at large.[225]

The main advantage of this model is its focus on the incentives of the actual actors who need to make decisions in real time as new opportunities and risks that involve users' data present themselves. Creating an ex ante incentive for these actors to act responsively is crucial in the dynamic and rapidly changing

---

[222] *See* discussion *supra* Section II.A.

[223] *See, e.g.*, Joel R. Reidenberg, *Setting Standards for Fair Information Practice in the U.S. Private Sector*, 80 IOWA L. REV. 497, 536 (1995) ("The private sector has precisely the type of dossiers that the public has long feared government would abuse.").

[224] *See* Chan, *supra* note 197.

[225] On the potential distinction between the two issues, see *supra* Section II.A.

landscape of social networking. Indeed, the data-sharing economy develops rapidly, from mere verbal communication between users to sharing of physical characteristics (such as pulse and breathing) and to the unknown future of what today may belong in science fiction books. These challenges will be better addressed if the relevant actors in the market are incentivized to tackle them responsively ex ante than if society attempts to identify the harms and remedy them ex post. Such an approach will allow social networking to constantly evolve and grow, while maintaining users' integrity and trust. Once implemented successfully, this approach can also be adopted to other technological fields that are emerging and ever-changing.