Boston College Law Review

Volume 57 | Issue 5 Article 6

11-30-2016

Corporate Privacy Failures Start at the Top

Victoria L. Schwartz
Pepperdine University School of Law, victoria.schwartz@pepperdine.edu

Follow this and additional works at: http://lawdigitalcommons.bc.edu/bclr

 Part of the Business Organizations Law Commons, Internet Law Commons, Law and Society Commons, and the Privacy Law Commons

Recommended Citation
Victoria L. Schwartz, *Corporate Privacy Failures Start at the Top*, 57 B.C.L. Rev. 1693 (2016), http://lawdigitalcommons.bc.edu/bclr/vol57/iss5/6

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

CORPORATE PRIVACY FAILURES START AT THE TOP

VICTORIA L. SCHWARTZ*

Abstract: With the rise of big data, numerous corporations are in the privacy business. Yet even corporations not directly in the privacy business must also make important decisions potentially impacting the privacy of their employees, consumers, and shareholders. A wide consensus of scholars and commentators has agreed that corporations fail to adequately protect privacy. The existing scholarship has largely focused on demand-side market failures to explain this privacy failure phenomenon. This Article offers a supply-side market distortion theory that reinforces the existing demand-side explanations to better account for corporate privacy failures. Under this supply-side theory, extensive corporate disclosure requirements, including the real possibility of disclosure of personal information about corporate executives, as well as a legally protected interest by the media in the personal lives of corporate executives combine to cause the pool of corporate executive candidates to sort in favor of individuals who do not themselves highly value privacy. This sorting effect can prevent the corporation from being able to properly anticipate and respond to various privacy issues. Recognition of this Article's supply-side market distortion theory allows a shift away from a singular view of the corporate privacy problem as a consumer-driven market failure. This enables identifying counterbalancing steps that can help offset the corporate-side sorting effect such as allowing corporate executives to negotiate individualized disclosure policies, and adding chief privacy officers to conceptions of good corporate governance in order to ensure that there is someone in the corporate leadership tasked with raising privacy concerns.

© 2016, Victoria L. Schwartz. All rights reserved.

* Associate Professor, Pepperdine University School of Law. Thank you to Geoffrey Lee, Caley Turner and Amy Rose for their editing and research assistance. I would also like to give thanks to Afra Afsharipour, Ian Ayres, Jordan Barry, Rich Chen, Lynne Dallas, Joshua Fairfield, Darren Good, David Han, Chris Hoofnagle, Christine Jolls, Alvin Klevorick, Adriaan Lanni, Yoon-Ho Alex Lee, Tom Lin, Yair Listokin, Michael Livermore, Greg McNeal, Derek Muller, Elizabeth Pollman, Lisa Ramsey, Neil Richards, Megan Shaner, Lior Strahilevitz and participants at the Harvard/Stanford/Yale Junior Faculty Forum, Privacy Law Scholars Conference-Amsterdam, University of San Diego Faculty Colloquium, UNH Law's Fifth Annual IP Scholars' Roundtable, National Business Law Scholars Conference and Law & Society 2015 Annual Meeting for their helpful comments.

INTRODUCTION

The corporate track record on privacy is troubling. There are countless examples of corporations neglecting to protect, failing to consider, or in some cases even intentionally violating the privacy of their consumers, employees, and even occasionally their shareholders. As a consequence, corporations have developed a well-earned reputation of inadequately protecting privacy.

In recent years, numerous corporations have even been forced to issue apologies and explanations regarding their treatment of privacy in response to consumer outrage and backlash.[1] This has prompted the question of why each corporation failed to correctly anticipate the privacy problem in the first case. Such companies as Yahoo and Google have repeatedly faced privacy lawsuits.[2] Famously, in 1999, Sun Microsystems CEO Scott McNealy told reporters and analysts that their focus on consumer privacy issues is a "red herring."[3] "You have zero privacy anyway," McNealy proclaimed, "[g]et over it."[4]

Furthermore, in an Internet-of-things world in which modern technology is rapidly being integrated into everyday objects, this corporate privacy failure phenomenon is not limited to dedicated technology companies. Traditional corporations have also found themselves facing scrutiny for failing to protect

---

[1] *See, e.g.*, Reed Albergotti, *Furor Erupts Over Facebook's Experiment on Users*, WALL STREET J. (June 30, 2014, 9:55 PM), http://www.wsj.com/articles/furor-erupts-over-facebook-experiment-on-users-1404085840 [https://perma.cc/K6HD-2BCG] (reporting consumer outrage after Facebook invaded users' privacy by conducting experiments that attempted to manipulate the users' emotions); Tamara Chuang, *Playing Pokemon Go? Here's How to Stay Safe*, DENVER POST (July 15, 2016, 4:56 PM), http://www.denverpost.com/2016/07/15/pokemon-go-safety-online/ [https://perma.cc/NX8T-JFA4] (reporting Niantic Inc.'s apology for Pokemon Go's Google account access controversy and highlighting other privacy concerns with the hit app); Stephanie Mlot & Chloe Albanesius, *Spotify CEO Apologizes for Privacy Policy Confusion*, PC MAG. (Aug. 21, 2015, 11:05 AM), http://www.pcmag.com/article2/0,2817,2489855,00.asp [https://perma.cc/7ZLA-TGNV] (addressing consumer backlash over Spotify's new privacy policy and the CEO's subsequent apology); *Notice of Data Breach*, OMNI HOTELS & RESORTS (July 8, 2016), https://www.omnihotels.com/notice [https://perma.cc/65FL-RA43] (apologizing for a breach of customer financial data and offering one free year of identity theft protector for affected guests); Keith Wagstaff, *Uber Battles Privacy Concerns Over 'God View' Tool*, NBC NEWS (Nov. 19, 2014, 10:51 AM), http://www.nbcnews.com/tech/tech-news/uber-battles-privacy-concerns-over-god-view-tool-n251691 [https://perma.cc/96DF-UCL8] (discussing consumer concern and company responses after Uber used tracking tools without users' consent).

[2] *See, e.g.*, Sooraj Shah, *Yahoo to Face Legal Action Over Email Spying*, COMPUTING (May 28, 2015), http://www.computing.co.uk/ctg/news/2410386/yahoo-to-face-legal-action-over-email-spying [https://perma.cc/TM6X-Y23F]; David Streitfeld, *Google to Pay $7M in Street View Privacy Case*, BOS. GLOBE (Mar. 13, 2013), https://www.bostonglobe.com/business/2013/03/12/google-pay-million-for-scooping-data-street-view-production/25ehHQyeAEkh6LaAIot5fM/story.html [https://perma.cc/LRK9-MACJ].

[3] Polly Sprenger, *Sun on Privacy: 'Get Over It,'* WIRED (Jan. 26, 1999), http://archive.wired.com/politics/law/news/1999/01/17538 [https://perma.cc/5NWE-NDLW].

[4] *Id.*

privacy. For example, the automobile industry has been under attack for failing to protect consumer privacy as it works to integrate modern technology into the automobile.[5] Similar privacy concerns have arisen in the toy industry, where Mattel has received criticism for the privacy-invasive way it integrated modern voice-recognition technology into its "Hello Barbie" doll, causing the doll to be insultingly nicknamed the "Eavesdropping Barbie."[6]

One of the more newsworthy examples of corporate failures with regard to employee privacy involved AOL CEO Tim Armstrong violating the privacy of two of AOL's employees in February 2014. While attempting to defend AOL's decision to make changes to its retirement policies in a town-hall style meeting with employees, Armstrong revealed that AOL had two employees with "distressed babies" that cost the company one million dollars each in healthcare costs.[7] Armstrong subsequently apologized.[8] Although it isn't clear whether Armstrong's statements violated existing privacy laws such as the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"),[9] his statements suggested a disregard for the privacy of his employees and caused widespread outrage.[10]

Although Armstrong's comments made headlines, far more ordinary and unpublicized corporate workplace invasions of privacy occur every day. Corporations invade the privacy of their employees as the result of medical testing, drug testing, corporate wellness programs, personality testing, and

---

[5] *See, e.g.*, Aaron M. Kessler, *Report Sees Weak Security in Cars' Wireless Systems*, N.Y. TIMES (Feb. 8, 2015), http://www.nytimes.com/2015/02/09/business/report-sees-weak-security-in-cars-wireless-systems.html [https://perma.cc/78GA-3K5S].

[6] Sarah Halzack, *Privacy Advocates Try to Keep 'Creepy,' 'Eavesdropping' Hello Barbie from Hitting Shelves*, WASH. POST (Mar. 11, 2015), https://www.washingtonpost.com/news/the-switch/wp/2015/03/11/privacy-advocates-try-to-keep-creepy-eavesdropping-hello-barbie-from-hitting-shelves/ [https://perma.cc/B5FK-HSWL].

[7] Jia Lynn Yang, *AOL Chief Cuts 401(k) Benefits, Blames Obamacare and Two "Distressed Babies,"* WASH. POST (Feb. 7, 2014), http://www.washingtonpost.com/news/wonkblog/wp/2014/02/06/aol-chief-cuts-401k-benefits-blames-obamacare/ [https://perma.cc/5KVB-ET9Z]. Armstrong stated that "[w]e had two AOL-ers that had distressed babies that were born that we paid a million dollars each to make sure those babies were OK in general." *Id.* Armstrong was attempting to justify a reduction in AOL's 401(k) benefits by explaining that the company was incurring costs in other benefit areas. *Id.*

[8] Michelle Miller, *AOL CEO Tim Armstrong Apologizes for "Distressed Babies" Remarks*, CBS NEWS (Feb. 10, 2014, 7:02 PM), http://www.cbsnews.com/news/aol-ceo-tim-armstrong-apologizes-for-distressed-babies-remarks/ [https://perma.cc/F2JV-TAV9].

[9] Dan Munro, *Did AOL CEO Tim Armstrong Violate HIPAA?*, FORBES (Feb. 10, 2014, 3:22 PM), http://www.forbes.com/sites/danmunro/2014/02/10/did-aol-ceo-tim-armstrong-violate-hipaa/#2125ce9f6088 [https://web.archive.org/web/20151231002657/http://www.forbes.com/sites/danmunro/2014/02/10/did-aol-ceo-tim-armstrong-violate-hipaa/].

[10] *See, e.g.*, *id.*; Natasha Singer, *Revelations by AOL Boss Raise Fears Over Privacy*, N.Y. TIMES (Feb. 10, 2014), http://www.nytimes.com/2014/02/11/business/media/revelations-by-aol-boss-raise-fears-over-privacy.html [https://perma.cc/6WLL-BGQG].

workplace surveillance programs ranging from monitoring e-mail to GPS trackers.

Even shareholders are not immune from the corporate privacy failure phenomenon. Original New York Stock Exchange member General Electric sent a supposedly anonymous survey to shareholders of its subsidiary GE Investments, asking the shareholders to rate different aspects of the company.[11] The shareholders were not informed that the return envelopes were coded such that the responses could be matched to names.[12] By not asking shareholders to input their names and addresses, the company apparently hoped that, believing their responses were anonymous, the shareholders would agree to answer such personal questions as what percentage of their investments was managed by the company.[13]

These sorts of privacy failure stories are neither unusual nor new. Over two decades ago, in his study of corporate privacy practices, management scholar H. Jeff Smith recounted some of the more notable corporate privacy problems of the 1990s.[14] To put it bluntly, his conclusions were ugly. He found that corporate privacy practices received systematic inattention and a lack of resources. Privacy policies largely didn't exist at all, and if they did, they were often ignored. Smith found that organizations he studied tended to be reactive on privacy issues, and concluded that "most executives wait until an external threat forces them to consider their privacy policies."[15]

In light of this track record, it is unsurprising that scholars have not been impressed with corporate treatment of privacy. One scholar noted, "[L]eaving privacy controls in individual companies' hands has proven to be a longstanding fox-in-the-henhouse type failure."[16] A second scholar concurred, "[C]orporate America and Fortune 500 companies . . . view personal information as a commodity and believe that it is their corporate right to exploit and manipulate personal information as they see fit."[17]

The existing scholarly explanations for this descriptive claim regarding the inadequacies of corporate treatment of privacy can be broadly categorized

---

[11] Robert O'Harrow, Jr., *Survey Says: You're Not Anonymous*, WASH. POST (June 9, 1999), http://www.washingtonpost.com/archive/business/1999/06/09/survey-says-youre-not-anonymous/e2b27c03-f0fb-457d-bd76-5398d2df6ded/ [https://perma.cc/63T8-LMFY].

[12] *Id.*

[13] *Id.*

[14] H. JEFF SMITH, MANAGING PRIVACY: INFORMATION TECHNOLOGY AND CORPORATE AMERICA 1–14 (1994); *see also* Kenneth A. Bamberger & Deirdre K. Mulligan, *Privacy on the Books and on the Ground*, 63 STAN. L. REV. 247, 249 (2011) (discussing Smith's findings).

[15] SMITH, *supra* note 14, at 93.

[16] Joshua A.T. Fairfield, *Mixed Reality: How the Laws of Virtual Worlds Govern Everyday Life*, 27 BERKELEY TECH. L.J. 55, 106 (2012).

[17] Marcy E. Peek, *Information Privacy and Corporate Power: Towards a Re-Imagination of Information Privacy Law*, 37 SETON HALL L. REV. 127, 138 (2006).

within two demand-side consumer-centric camps. First, one group of scholars concludes that corporations do not care about privacy because consumers do not care about privacy, or at least do not care about privacy as much as other priorities.[18] For this camp, there is not a real privacy problem; corporations aren't protecting privacy because privacy isn't something that consumers have decided needs protection. For the second group of scholars, corporations do not care about privacy because there is some sort of market failure in which consumers who do care about privacy are unable to make choices to express that preference in the market.[19] For this group, the demand-side privacy market failure likely requires legal intervention to correct for that failure.

This Article adds an additional supply-side corporate market distortion theory to supplement the prevailing demand-side accounts explaining why corporations inadequately consider and protect privacy. This theory posits that as a result of various systemic legal and societal failures to protect the personal privacy of high-level corporate executives, individuals who place a high value on their own privacy are less likely to pursue high-level executive positions at publicly traded corporations. As a result of this sorting effect, those remaining candidates who do pursue the high-level corporate executive positions are, on the whole, less likely to highly value their own privacy. This reduced personal privacy preference may cause corporate executives to undervalue or not even recognize the privacy implications of their business decisions. This is more likely when the privacy issue is not squarely presented, but arises in a seemingly innocuous product design decision. Nevertheless, these low-privacy preference individuals are responsible for making important corporate privacy decisions, as well as setting the tone for lower-level decisionmakers regarding what values the corporation ought to prioritize. As such, the individual privacy preferences of senior-level corporate executives can impact corporate behavior on privacy issues. Recognizing this supply-side story does not undermine or

---

[18] *See, e.g.*, JEFFREY ROSEN, THE UNWANTED GAZE: THE DESTRUCTION OF PRIVACY IN AMERICA 181 (2000) ("Most people don't care about privacy until they have something to hide, and there's no reason to believe that consumers wouldn't voluntarily transfer property rights in their personal data to commercial Web sites in exchange for product discounts and other conveniences."); Ira S. Rubinstein, *Regulating Privacy by Design*, 26 BERKELEY TECH. L.J. 1409, 1412 (2011) (listing possible reasons for a low demand in products and services with strong privacy safeguards including consumers not caring very much about privacy).

[19] *See, e.g.*, Fairfield, *supra* note 16, at 106–07 (noting that there is a corporate privacy-market failure because the transaction costs of privacy have been placed on consumers); Andrea M. Matwyshyn, *Privacy, The Hacker Way*, 87 S. CAL. L. REV. 1, 35 (2013) (noting the impossibility of expecting consumers to read large numbers of privacy policies); Peek, *supra* note 17, at 164 (identifying a corporate privacy-market failure resulting from the fallacy of consumer choice because consumers must consent to a privacy policy or not do business with an entire industry); Rubinstein, *supra* note 18, at 1432 (noting the market failure within the privacy market resulting from information asymmetries).

replace, but rather supplements and demonstrates the salience of the demand-side privacy problems.

The Article proceeds in four parts. Part I discusses the systemic studies, academic scholarship, and real-world examples demonstrating the widespread failure on the part of corporations to protect privacy.[20] It then addresses the existing consumer-centric explanations scholars have offered to account for these privacy failures.[21] Part II presents the additional supply-side corporate market-distortion hypothesis as an additional theory for why corporations fail to adequately protect privacy.[22] This Part identifies the features of the legal system and society more generally that cause a sorting effect by which individuals who care about privacy do not choose to become corporate executives.[23] It then explores the implications of that sorting on corporate privacy decision making.[24] Part III offers some corporate-side solutions that would help counter the corporation-side cause of the privacy problem such as allowing corporate executives to negotiate disclosure policies covering the corporate disclosure of their personal information and adopting chief privacy officers ("CPOs") as a part of good corporate governance.[25] This Article then concludes by setting out a roadmap for future empirical work that can test the some of the assumptions in the theoretical hypothesis offered in this Article.

I. Systematic Corporate Privacy Failures

For decades, scholars and commentators have agreed that corporations do not adequately prioritize privacy.[26] This consensus is reinforced by numerous examples and studies of corporations failing to adequately protect, neglecting to recognize, and even intentionally invading the privacy of their corporate constituents. Although big data and technology advancements have changed the ease and frequency with which this corporate privacy failure phenomenon occurs, the corporate privacy failures themselves are not new. Corporations have consistently demonstrated that they do not prioritize privacy.[27]

---

[20] *See infra* notes 26–89 and accompanying text.
[21] *See infra* notes 90–126 and accompanying text.
[22] *See infra* notes 127–255 and accompanying text.
[23] *See infra* notes 140–193 and accompanying text.
[24] *See infra* notes 194–255 and accompanying text.
[25] *See infra* notes 256–295 and accompanying text.
[26] *See infra* notes 28–39 and accompanying text.
[27] Corporations do at times care about their own corporate privacy to the extent that such a thing exists, but that is a conceptually different concept. For more about corporate privacy, see generally Elizabeth Pollman, *A Corporate Right to Privacy*, 99 Minn. L. Rev. 27 (2014).

A. Scholars Recognize the Corporate Privacy Failure

A strong consensus has developed that corporations do not make privacy a priority. As Marcy Peek describes, "[I]t is the entirety of corporate America and Fortune 500 companies that view personal information as a commodity and believe that it is their corporate right to exploit and manipulate personal information as they see fit."[28] Prominent sociologist Amitai Etzioni agrees with this view of corporations as a privacy threat, and that as a result, "[I]t is no longer possible to protect privacy by only curbing the State."[29] Similarly, Avidan Cover writes about the dangers of a system that relies on corporations to assert privacy rights against the government.[30] As Joshua Fairfield eloquently puts it, "[L]eaving privacy controls in individual companies' hands has proven to be a longstanding fox-in-the-henhouse type failure."[31]

Scholars have recognized this corporate privacy failure in a wide variety of industries and contexts. For example, Katrin Byford explains that the realm of cyberspace has the potential "to have distinct Orwellian overtones—with the notable difference that the primary threat to privacy comes not from government, but rather from the corporate world."[32] Similarly, Derek Witte discusses the problems associated with data mining and sharing in the context of large Internet companies.[33] He warns:

> Citizens who value privacy should be nervous, for the companies that want to store personal data on their "big iron" and simply allow users to visit the documents they create, spreadsheets they build, and books they buy are the same companies that force customers to agree to terms of service that will give these giant corporations a right to read, use, and pilfer customer data for value.[34]

---

[28] Peek, *supra* note 17, at 138.

[29] Amitai Etzioni, *The Privacy Merchants: What Is to Be Done?*, 14 U. PA. J. CONST. L. 929, 950–51 (2012).

[30] Avidan Y. Cover, *Corporate Avatars and the Erosion of the Populist Fourth Amendment*, 100 IOWA L. REV. 1441, 1445 (2015).

[31] Fairfield, *supra* note 16, at 106.

[32] Katrin Schatz Byford, *Privacy in Cyberspace: Constructing a Model of Privacy for the Electronic Communications Environment*, 24 RUTGERS COMPUTER & TECH. L.J. 1, 50 (1998).

[33] Derek S. Witte, *Bleeding Data in a Pool of Sharks: The Anathema of Privacy in a World of Digital Sharing and Electronic Discovery*, 64 S.C. L. REV. 717, 729 (2013).

[34] *Id.*; *see also* Derek S. Witte, *Privacy Deleted: Is It Too Late to Protect Our Privacy Online?*, J. INTERNET L., Jan. 2014, at 1, 17 ("Google reached a compromise with the FTC under . . . threat of an enforcement action. As a result, Google revised its privacy policy . . . . The synthesized policy, however, revealed that Google had no interest in maintaining consumer privacy.").

More generally, Daniel Solove has described the privacy harms that occur at the hands of corporations who gather large amounts of consumer data.[35] Solove describes the "thoughtless and irresponsible ways that bureaucracies use personal information and their lack of accountability in using and protecting the data."[36] In addition to the inadequate formal privacy policies, Solove also criticizes the "irresponsible and careless uses of personal information" and the "complete lack of care and accountability by the corporations collecting the data."[37] These scholars are just a few examples of the various voices agreeing that corporations do not prioritize privacy.[38] There is a notable absence of scholarly voices arguing otherwise.[39]

---

[35] *See* Daniel J. Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, 53 STAN. L. REV. 1393, 1424–30 (2001).

[36] *Id.* at 1428.

[37] *Id.* at 1428–29.

[38] *See* Mike Hatch, *The Privatization of Big Brother: Protecting Sensitive Personal Information from Commercial Interests in the 21st Century*, 27 WM. MITCHELL L. REV. 1457, 1485–86 (2001) (describing a phenomenon whereby "commercial interests have collected massive amounts of information about individuals which is used readily to encroach on consumer privacy. The wide dissemination of such information and purchasing habits has harmed consumers by creating an environment susceptible to identity theft and unauthorized charges. There is also a growing perception that the financial market is less secure and that partnerships between financial institutions and telemarketers may destabilize the financial industry."); Larry O. Natt Gantt, II, *An Affront to Human Dignity: Electronic Mail Monitoring in the Private Sector Workplace*, 8 HARV. J. L. & TECH. 345, 348 (1995) ("[E]mployees must rely on employer self-regulation to protect their privacy interests. This solution is unacceptable because employers often believe they have significant incentives to marginalize the protection of employee privacy. Consequently, American businesses have largely failed to revise their in-house privacy policies despite their increasing use of electronic monitoring. This enlarging gap between employee privacy interests and employer monitoring policies is undoubtedly reflected in the marked increase in employee suits alleging invasion of privacy by employers."); Joel R. Reidenberg, *Setting Standards for Fair Information Practice in the U.S. Private Sector*, 80 IOWA L. REV. 497, 498 (1995) (describing the business community's attempts at developing "appropriate business practices for self-regulation" of the treatment of personal information as having "broken down"). *See generally* Oscar H. Gandy, Jr., *Legitimate Business Interest: No End in Sight? An Inquiry into the Status of Privacy in Cyberspace*, 1996 U. CHI. LEGAL F. 77 (1996) (arguing that "businesses have an interest in being informed about individuals because of the strategic importance of that information" as a means of attempting to control decisions those individuals make as citizens, consumers, and employees).

[39] At most, some scholars have demonstrated that corporations increasingly recognize that there can be public relations reasons to at least appear to care about privacy. *See, e.g.*, Nicole A. Ozer, *Putting Online Privacy Above the Fold: Building a Social Movement and Creating Corporate Change*, 36 N.Y.U. REV. L. & SOC. CHANGE 215, 239–40 (2012) (pointing out that "many companies are taking steps to demonstrate that they value user privacy, including backtracking from changes that generate significant public protest. . . . In fact, online privacy has become such a central issue in the business world that Facebook hired a public relations firm to pitch stories critical of its competitor, Google, in order to shift the spotlight away from Facebook's privacy issues"). It is certainly possible, however, that assuming an optimal level of privacy and that corporations can either over-protect or under-protect privacy relative to that baseline optimal level, that it only makes the news when corporations under-protect privacy and not when they over-protect. If that were true, however, one would think that corporations would have incentives to better publicize that fact in some way.

B. Studies Documenting Corporate Privacy Problems

The scholarly consensus regarding corporate privacy problems has been reinforced by studies systematically documenting the corporate treatment of privacy. In a 1993 study, Smith investigated corporate privacy practices. He interviewed executives, managers, and employees of the studied companies, conducted written surveys of employees, and spoke with privacy and consumer advocates and industry observers.[40] Smith cataloged extensive problems with corporate privacy. He found that corporations systematically lacked privacy policies, and where such policies existed, they were typically ignored.[41] Smith discovered that the organizations that he studied were reactive with regard to privacy issues, and that "most executives wait until an external threat forces them to consider their privacy policies."[42] He determined that all the various companies followed a similar approach to the process of privacy policy-making, an approach that he described as "a wandering and reactive one."[43]

Specifically, Smith described high-profile examples of corporate privacy failures of that era. For instance, Blockbuster video had planned to sell mailing lists of its customers.[44] It only retracted the plan after a privacy backlash from its customers.[45] Similarly, executives of Lotus Development Corporation and Equifax Marketing Decision Systems cancelled the release of a product that would have given information about American households to businesses for use in direct marketing.[46] They backpedaled following negative press coverage and subsequent customer requests to be deleted from the database.[47]

The banking industry examined at the time fared no better at protecting customer privacy. Smith found that two of the banks studied both had plans to collect extensive computerized information about their customers.[48] The banks' plan was to gather that data using both the forms customers submitted when they opened accounts as well as automation systems in which bank employees used casual conversations with customers to gather and then

---

[40] SMITH, *supra* note 14, at 15–17.

[41] *Id.* at 4, 135–36. There are some sample bias reasons to think that the actual privacy practices at the time may be even worse than Smith's study revealed. Companies were given the opportunity to opt-out of his study, and a number of companies did so. *Id.* at 51–54 (explaining the voluntary nature of the study and acknowledging that certain companies refused to participate). Logically, the companies who chose not to participate may have had even worse privacy policies than the companies who agreed to participate.

[42] *Id.* at 93.

[43] *Id.* at 55.

[44] *Id.* at 2.

[45] *Id.*

[46] *Id.*

[47] *Id.*

[48] *Id.* at 102.

manually enter personal customer information such as the number of children, whether the home was rented or owned, and household income.[49] The banks at the time had no privacy policies regarding this sort of collection of information.[50] One bank executive explained that the goal was to "get any information you can *from* people and *about* people."[51] Another banking executive confessed:

> The truth is that almost any officer of the bank (especially, one with lending authority) can get at any information in the computer system . . . . I never promise my customers total privacy, because I know I cannot deliver it. A lot of them assume they are entering into a confidential arrangement, however, and I don't tell them otherwise unless they ask.[52]

The executive explained that ensuring more customer privacy would create an increased administrative burden.[53]

More recently, Kenneth A. Bamberger and Deirdre K. Mulligan set out to update Smith's "landmark" study of corporate privacy practices and his "grim" conclusions regarding "how corporations actually manage privacy and what motivates them," or what they call "privacy on the ground."[54] Their published initial findings of their empirical research found a far different picture than Smith's disastrous findings. Within the corporations they studied, they found a "shift" in the treatment of privacy.[55] Their subsequent, more comprehensive book on corporate privacy behavior in the United States and Europe similarly found that the corporate management of privacy "has undergone a profound transformation."[56]

Despite these rosier findings, Bamberger and Mulligan's research does not purport to suggest that corporate privacy problems have disappeared. This is because their self-described methodology involved qualitative interviews with CPOs who were "identified as industry leaders by their peers."[57] In other words, the sample was intentionally selected from the best in class with regard

---

[49] *Id.*
[50] *Id.*
[51] *Id.*
[52] *Id.* at 127.
[53] *Id.*
[54] Bamberger & Mulligan, *supra* note 14, at 249.
[55] *Id.* at 251 (describing coherence across the interviewed CPOs with regard to "a profound shift in the definition of privacy and its treatment").
[56] KENNETH A. BAMBERGER & DEIRDRE K. MULLIGAN, PRIVACY ON THE GROUND: DRIVING CORPORATE BEHAVIOR IN THE UNITED STATES AND EUROPE 8 (2015) (contending that the "privacy landscape today would be unrecognizable" to the survey respondents in Smith's study).
[57] Bamberger & Mulligan, *supra* note 14, at 249.

to corporate treatment of privacy. Therefore, as they warn, the small sample and choice of identified industry leaders means that the conclusions that can be drawn "are necessarily limited" and "do not . . . provide evidence of corporate attitudes towards privacy more generally."[58] As discussed further subsequently, to the extent that any conclusions can be drawn from their sample, their study is actually consistent with the theory offered in this Article by demonstrating that the characteristics of those corporations that have more successful privacy reputations match those that would be predicted based on the supply-side market distortion hypothesis.[59]

Studies have also found corporate privacy failures with employee privacy. A study of eighty-four Fortune 500 companies representing over 3.2 million employees conducted in 1995, for example, found that the companies studied failed to adequately protect employee information.[60] The study found that 42% of corporations did not have a policy for conducting periodic evaluations of their personnel record-keeping systems, and had not designated an executive-level individual to be responsible for maintaining privacy safeguards for employment record-keeping practices.[61] Seventy-five percent of the companies surveyed answered that they routinely "check, verify, or supplement" information about their employees beyond what the employees voluntarily provided.[62] Nearly half did not inform workers they were gathering the information.[63] Similarly, a 2007 study of employer monitoring and surveillance practices found that employers use a variety of technological tools to routinely engage in monitoring and surveillance of employees.[64] Computer monitoring took many forms, with 45% of employers tracking content, keystrokes, and time spent at the keyboard.[65] Forty-three percent of companies studied monitored e-mail, with 96% of those tracking external incoming and outgoing messages.[66] An earlier study "found a positive correlation between the size of the company and its level of monitoring and surveillance, with the largest companies conducting the most surveillance."[67] A 2010 study found that 37% of U.S. companies with one thousand or more employees employed staff

---

[58] *Id.* at 252.

[59] *See infra* notes 127–255 and accompanying text.

[60] David F. Linowes & Ray C. Spencer, *How Employers Handle Employees' Personal Information: Report of a Recent Survey*, 1 EMP. RTS. & EMP. POL'Y J. 153, 156 (1997).

[61] *Id.* at 170.

[62] *Id.* at 159.

[63] *Id.*

[64] *2007 Electronic Monitoring & Surveillance Survey*, EPOLICY INST. (2007), http://www.epolicyinstitute.com/2007-survey-results [https://perma.cc/T8QS-5LAD].

[65] *Id.*

[66] *Id.*

[67] *See* Reginald C. Govan & Freddie Mac, *Workplace Privacy*, *in* 33RD ANNUAL INSTITUTE ON EMPLOYMENT LAW 245, 251 (Practising Law Inst., 2004).

whose job it is to either read or analyze outbound e-mail and 48% performed regular audits of the outbound e-mail content.[68] In summary, studies consistently support the scholarly claim that corporations do not prioritize the privacy of their corporate constituents.

C. Contemporary Corporate Privacy Failure Examples

Although some laws have changed[69] by providing more protection for consumers and employees from certain limited types of privacy invasions,[70] the news continues to be littered with countless examples of corporate privacy invasions with regard to all types of corporate constituents as well as all types of industries. For example, privacy advocates have recently requested a closer look at consumer gadgets that are "always on," including Microsoft's Kinect controller, Amazon's Echo assistant, and smart-televisions from Samsung and others.[71] The Electronic Privacy Information Center has asked regulators to consider how data from such devices is collected and stored, in addition to whether consumers truly understand what data is being collected.[72]

Some of these concerns about corporate treatment of consumer privacy have led to legal action. Yahoo is facing a class action lawsuit over claims that it accessed and analyzed the content of e-mails sent to Yahoo Mail users from non-Yahoo Mail accounts and used the data to boost its advertising revenue.[73] Google has been involved in numerous privacy lawsuits.[74] In 2013, Google agreed to pay $7 million for secretly collecting personal information including e-mails and medical and financial records by data-scooping from millions of unencrypted wireless networks as it cruised by to create its Street View.[75] The

---

[68] PROOFPOINT, OUTBOUND EMAIL AND DATA LOSS PREVENTION IN TODAY'S ENTERPRISE 6 (2010).

[69] Whereas some privacy laws do exist, many scholars believe that the law is far behind technological developments in protecting privacy. There are systemic reasons similar to those discussed in this Article to support a theoretical hypothesis that politicians are also less likely to care about their own privacy, and consequently less likely to press for and prioritize privacy laws. I pursue this separate but related theory in a companion paper, tentatively titled *The Nation's Privacy Problems Start with Elected Politicians*.

[70] *See, e.g.*, Genetic Information Nondiscrimination Act of 2008, Pub. L. No. 110-233, 122 Stat. 881 (codified as amended in scattered sections of 29 and 49 U.S.C.). (protecting against employment discrimination based on genetic information).

[71] Hayley Tsukayama, *Privacy Advocates Ask Regulators to Take a Closer Look at Gadgets That Are 'Always on,'* WASH. POST (July 10, 2015), https://www.washingtonpost.com/news/the-switch/wp/2015/07/10/privacy-advocates-ask-regulators-to-take-a-closer-look-at-gadgets-that-are-always-on/ [https://perma.cc/Z66J-HUQ5].

[72] *Id.*

[73] Shah, *supra* note 2.

[74] Streitfeld, *supra* note 2.

[75] *Id.*

company previously paid $22.5 million to settle FTC charges that it bypassed the privacy settings on Apple's Safari browser.[76]

Nor are these corporate privacy failures with regard to consumers limited to the Silicon Valley high-tech companies. Rather, as traditional industries begin to integrate technology in various ways into more traditional products, they too increasingly face problems with adequately protecting privacy. More traditional corporations, such as the automobile industry, have recently faced scrutiny both for "serious gaps" in protecting customer privacy from hackers in vehicles using wireless technology and for the manner in which they track driver behavior, and collect, transmit and store that information.[77]

These concerns become more high stakes when the privacy of children is involved. Privacy advocates have criticized traditional toy company Mattel's Hello Barbie, which is equipped with voice-recognition software that permits the doll to "listen" to the child's words and respond appropriately, including learning information over time and adjusting to new topics.[78] The doll "listens" by sending audio recordings of the child over the Internet to a server where the child's conversations are recognized and processed.[79] This invasion of a child's personal conversations with his or her doll has caused privacy advocates to disparagingly call the doll Eavesdropping Barbie.[80]

The story is similar with regard to companies invading employee privacy. Myrna Arias recently brought the reality of employer GPS tracking into the news.[81] According to her lawsuit, Arias was fired after she disabled the GPS application on her company-issued smartphone after she discovered that her employer could track her even when she was off-duty.[82] Such GPS tracking has long been common in company-owned vehicles, but now has increasingly been used through smartphones. Other employee invasions of privacy include drug testing programs, personality testing, intrusive wellness programs, computer, e-mail and technological monitoring, and employer control of off-duty life.[83]

---

[76] *Id.*

[77] Kessler, *supra* note 5.

[78] Halzack, *supra* note 6.

[79] *Id.*

[80] *Id.*

[81] Adriana Gardella, *Employer Sued for GPS-Tracking Salesperson 24/7*, FORBES (June 5, 2015, 10:57 AM), http://www.forbes.com/sites/adrianagardella/2015/06/05/employer-sued-for-gps-tracking-salesperson-247/#292a534536d4 [https://web.archive.org/web/20161021115009/http://www.forbes.com/sites/adrianagardella/2015/06/05/employer-sued-for-gps-tracking-salesperson-247/#23dee4525450].

[82] *Id.*

[83] *See generally* Victoria Schwartz, *Overcoming the Public-Private Divide in Privacy Analogies*, 67 HASTINGS L.J. 143, 161 (2015) (discussing workplace privacy problems).

In addition to these invasions of consumer and employee privacy, the news is also filled with examples of corporations failing to adequately protect consumer and employee privacy and therefore suffering data and security breaches. For example, after the widely publicized Sony breach, current and former employees sued alleging that Sony did not adequately protect employee data.[84] The hackers accessed data including the social security numbers of 47,000 current and former employees, and the medical information of some employees and their families.[85] Similar breaches have impacted companies in a variety of industries including graphics card company Nvidia,[86] health insurer Anthem,[87] home retailer Home Depot,[88] and discount retailer Target.[89] These anecdotal examples of corporate treatment of privacy reinforce the broader studies suggesting that corporations systematically fail to adequately address privacy concerns.

D. Conventional Explanation of Corporate Privacy Failures

As explained above, a consensus has developed among legal scholars concluding that corporations systematically fail with regard to the privacy of their constituents.[90] The existing scholarship seeking to offer an explanation

---

[84] Saba Hamedy & Meg James, *Sony Hit with Lawsuit by Former Employees Over Email Leaks*, L.A. TIMES (Dec. 16, 2014, 9:14 AM), http://www.latimes.com/entertainment/envelope/cotown/la-et-ct-sony-class-action-lawsuit-employees-20141215-story.html [https://perma.cc/TB8Z-L6K6].

[85] *Id.*

[86] Dave Lewis, *NVIDIA Corporate Network Breached*, FORBES (Dec. 29, 2014, 11:55 PM), http://www.forbes.com/sites/davelewis/2014/12/29/nvidia-corporate-network-breached/ [https://web.archive.org/web/20160324211658/http://www.forbes.com/sites/davelewis/2014/12/29/nvidia-corporate-network-breached/#2fd3216961be].

[87] Charles Ornstein, *Health Data Breaches Sow Confusion, Frustration*, USA TODAY (Apr. 14, 2015, 8:49 AM), http://www.usatoday.com/story/money/2015/04/14/hacking-health-data-privacy/25597337/ [https://perma.cc/G286-FGA7].

[88] *See* Elise Viebeck, *Home Depot Still Paying for Data Breach*, THE HILL (May 19, 2015, 12:45 PM), http://thehill.com/policy/cybersecurity/242510-home-depot-still-paying-for-data-breach [https://perma.cc/XRX2-YG8E].

[89] Robin Sidel, *Target to Settle Claims Over Data Breach*, WALL STREET J. (Aug. 18, 2015, 5:10 PM), http://www.wsj.com/articles/target-reaches-settlement-with-visa-over-2013-data-breach-1439912013 [https://perma.cc/5BBH-8RBM]. Disturbingly, the personal information of all federal employees, as well as one million former federal employees was recently stolen in the federal data breach of the Office of Personnel Management. Kate Vinton, *Federal Union Says OPM Data Breach Hit Every Single Federal Employee*, FORBES (June 11, 2015, 9:12 PM), http://www.forbes.com/sites/katevinton/2015/06/11/federal-union-says-opm-data-breach-hit-every-single-federal-employee/#72fd848dd1e4 [https://web.archive.org/web/20160506122526/http://www.forbes.com/sites/katevinton/2015/06/11/federal-union-says-opm-data-breach-hit-every-single-federal-employee/#28fac6013f4e]. Although raising many of the same troubling issues, that governmental breach is beyond the corporate scope of this Article.

[90] *See supra* notes 29–68 and accompanying text (noting studies that identify corporate privacy concerns as an issue in corporate America).

for the way in which corporations treat privacy largely can be categorized into two related demand-side schools of thought. Although these two groups of scholars disagree as to the precise cause of the corporate treatment of privacy, and disagree as to whether the situation should be normatively categorized as a "problem," both groups agree that the origin of the corporate privacy behavior occurs on the demand-side with the corporate constituents, most commonly the consumers.[91]

The first group of scholars within the demand-side explanation contends that the corporate treatment of privacy merely reflects the low level of privacy preferences held by consumers in the free market. This free market camp, sometimes referred to as the "libertarian privacy establishment"[92] or "market purists,"[93] believes that the free market can adequately encourage corporations to respect privacy rights. Under this school of thought, if consumers actually value privacy they will choose to give their business to companies that protect their privacy and the market will respond to that demand accordingly.[94] This will cause companies that fail to adequately protect consumer privacy to be driven from the marketplace. Conversely, under this neoclassical economic position, "If consumers choose to use services from companies that offer little to no privacy protection, that reveals a preference to spend little to nothing on (or looking for) privacy."[95] Therefore, according to this group of scholars, any examples of corporations invading or failing to protect consumer privacy merely reveal that the consumers prioritize other values such as efficiency, convenience, and personalization over protecting their privacy.[96]

---

[91] Although much of this scholarship takes place in the context of consumer privacy, presumably many of these scholars would make similar arguments with regard to the other corporate constituents such as employees and shareholders.

[92] Frank Pasquale, *Privacy, Antitrust, and Power*, 20 GEO. MASON L. REV. 1009, 1014 (2013).

[93] *See* Solove, *supra* note 35, at 1448.

[94] *See id.*

[95] Pasquale, *supra* note 92, at 1009 (describing, but not subscribing to this view); *see also* ROSEN, *supra* note 18, at 181 ("Most people don't care about privacy until they have something to hide and there's no reason to believe that consumers wouldn't voluntarily transfer property rights in their personal data to commercial Web sites in exchange for product discounts and other conveniences."); Rubinstein, *supra* note 18, at 1412 (listing possible reasons for a low demand in products and services with strong privacy safeguards including consumers not caring very much about privacy).

[96] *See, e.g.*, Irina D. Manta & David S. Olson, *Hello Barbie: First They Will Monitor You, Then They Will Discriminate Against You. Perfectly.*, 67 ALA. L. REV. 135, 138–39 (2015) (concluding that corporate behavior of monitoring users by means of consumer products such as Hello Barbie, "while regrettable at times—is almost inevitable, in large part because consumers so often are willing to trade being monitored for receiving products and applications that they like"); Maureen K. Ohlhausen & Alexander P. Okuliar, *Competition, Consumer Protection, and the Right [Approach] to Privacy*, 80 ANTITRUST L.J. 121, 122 (2015) (noting that certain advocates "believe that people are consciously choosing to trade at least some privacy for otherwise free and improved content and services").

This first camp contends that adequate market incentives already exist for corporations to protect privacy. They point to the existence of privacy-protecting technology in certain domains, such as the "In Private" browsing mode, as proof that in certain circumstances the privacy market is working.[97] They also call attention to various examples where corporations have reversed previous plans in response to a public outrage over privacy. For instance, Yahoo removed the ability to run a reverse telephone number search on its People Search site after it faced extensive privacy concerns.[98] Similarly, after facing a consumer backlash, Lexis-Nexis reversed its plans for a personal locator that would have provided the personal information, including the maiden names and social security numbers, of millions of people.[99] For this group, these sorts of corporate reversals demonstrate the success of the privacy market, rather than the existence of a problem. Consequently, they contend that the prevailing corporate privacy behavior does not require governmental reform or regulation because there is no problem—corporations are merely accurately identifying where weak privacy preferences in the market exist.[100]

Although the free market camp may be correct that sub-markets exist where privacy markets are robust, their account does not explain why such corporate reversals on privacy so frequently occur. Put differently, why aren't corporations better at anticipating the privacy consumer backlashes ex ante, given the negative public relations the policy reversals generate as well as the sunk costs the corporation is forced to absorb when it is forced to backpedal ex post? One way to view the project of this Article is that it allows those scholars that subscribe to the consumer free market camp to offer an explanation for that question.

By contrast, the second consumer-centric school of thought does not trust that the market is effective in protecting consumer privacy because there are a number of demand-side privacy market failures. For some of these scholars, the demand-side privacy market failure occurs in part because of "the lack of power that consumers have to determine the contractual terms governing the

---

[97] *See* Joshua A.T. Fairfield, *"Do-Not-Track" as Contract*, 14 VAND. J. ENT. & TECH. L. 545, 555 (2012) (describing, but not subscribing to this view).

[98] *See* Jerry Berman & Deirdre Mulligan, *Privacy in the Digital Age: Work in Progress*, 23 NOVA L. REV. 551, 564–65 (1999).

[99] See James P. Nehf, *Recognizing the Societal Value in Information Privacy*, 78 WASH. L. REV. 1, 59 (2003).

[100] *See* Solove, *supra* note 35, at 1448. *See generally* Kent Walker, *The Costs of Privacy*, 25 HARV. J.L. & PUB. POL'Y 87, 89–90 (2001) (advocating for a market approach to regulating privacy because an invasive regulatory regime would have "both direct and indirect costs to the individual consumer, reduce consumer choice, and inhibit the growing trend toward personalization and tailoring of goods and services").

sale or use of their data."[101] Even a consumer who wanted to take measures to protect his or her privacy, "would find the process nearly impossible,"[102] as a result of the diverse tracking methods companies have at their disposal.[103] For example, Solove uses a Kafka metaphor to describe "the power inequalities that pervade the world of information transfers between individuals and bureaucracies."[104]

In many industries, this power imbalance is exacerbated by the accumulation of market power that resembles the sort of power governed by antitrust law.[105] For example, consumers who wished to shop for pro-privacy terms for their search and social networking activities would find few options and little choice because the dominant providers remain vastly superior to any available alternatives, and therefore "see little to no reason to compete to improve their privacy practices when users are so unlikely to defect."[106] Consequently, the consumers are forced to consent to a particular type of privacy policy or not do business with an entire industry.[107]

Additionally, a number of scholars have recognized a potential privacy market failure resulting from information asymmetries and breakdowns. First, companies' privacy behavior is often not "readily observable" to consumers.[108] The privacy market does not adequately protect consumer privacy because so much data collection is done secretly.[109] And even where corporations draft and post privacy policies, they rarely provide useful information to consumers. Corporate privacy policies tend to make vague promises to protect and respect privacy.[110] Consumers rarely receive detailed explanations of what precisely the corporation will do with the information, what security measures are being taken, or what recourse they have if they disagree.[111] Instead, consumers must rely on the corporation to fulfill the lofty ideals in the privacy policies in a manner acceptable to the consumer.

Furthermore, the consumer often lacks the ability to know what is in the privacy policy in the first place. Even where they are available, and even if

---

[101] *See* Fairfield, *supra* note 97, at 551 (calling the lack of consumer contractual power "the heart of the current problem").

[102] *Id.* at 552.

[103] *Id.* at 554–67 (describing the various mechanisms of surveillance used by companies to invade privacy).

[104] Solove, *supra* note 35, at 1452.

[105] Pasquale, *supra* note 92, at 1022.

[106] *Id.*

[107] Peek, *supra* note 17, at 164.

[108] *See* Joseph Farrell, *Can Privacy Be Just Another Good?*, 10 J. TELECOMM. & HIGH TECH. L. 251, 256 (2012).

[109] Solove, *supra* note 35, at 1450.

[110] *Id.* at 1451.

[111] *Id.*

they contained useful information, it is implausible to expect consumers to read large numbers of privacy policies.[112] The existing privacy policy notice and opt-out regime involves excessively difficult transaction costs because consumers do not have "time or patience to read through cumbersome documents describing obscure rules for controlling data."[113] And many corporations change privacy policies frequently, making it harder for even the most diligent consumers to keep up with all the changes to these contracts of adhesion.[114]

Additionally, Joseph Farrell describes the potential for a "cynical market failure" in which consumers expect that a company will not protect privacy regardless of any policy, so they fail to reward companies regardless of the actual practice.[115] This creates a dysfunctional equilibrium in which companies have no incentive to protect privacy, which in turn reinforces the consumer expectations and exacerbates the situation.[116] Furthermore, Joshua Fairfield and Christoph Engel have explained that these consumer failures get exacerbated because privacy should be conceived as a public good with negative externalities rather than one held by individual consumers.[117] Consequently, the erroneous focus on individual consumer privacy at the expense of privacy's group dimension means that "individual consumers have been left to negotiate, unsuccessfully, with companies over the use of their data."[118]

Scholars also contend that the privacy market fails because consumers are unable to accurately price the value of their privacy. The value of a particular piece of information, such as a social security number, is not easy to ascertain for the individual consumer who cannot accurately capture the uncertain future uses that can be made with the data.[119] This challenge is further exacerbated by an aggregation problem. An individual may be willing to trade away numerous innocuous bits of information in different contexts. Each revelation itself is perfectly innocent, but when combined can offer extensive insights into the individual. As Julie Cohen explains, "[A] comprehensive collection of data

---

[112] Matwyshyn, *supra* note 19, at 35.

[113] LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 160 (1999).

[114] *See* Aaron E. Ghirardelli, *Rules of Engagement in the Conflict Between Businesses and Consumers in Online Contracts*, 93 OR. L. REV. 719, 720–21 (2015) (expressing concern regarding the "conflict between online businesses and consumers, in which Internet businesses use aggressive online adhesion contracts to create vast economic empires, and in which consumers have few resources to resist this virtual onslaught on their privacy and property rights").

[115] Farrell, *supra* note 108, at 257.

[116] *Id.*

[117] Joshua A.T. Fairfield & Christoph Engel, *Privacy as a Public Good*, 65 DUKE L.J. 385, 389–92 (2015).

[118] *Id.* at 392.

[119] Solove, *supra* note 35, at 1452.

about an individual is vastly more than the sum of its parts."[120] Therefore, in the context of each individual privacy-invading transaction, consumers cannot make a truly informed decision. Empirical research by Chris Hoofnagle and Jennifer Urban lends support to these demand-side market failure theories by showing that consumers had "fundamental misunderstandings about business practices, privacy protections, and restrictions upon the use of data" causing a distortion in the privacy market by leading "consumers to believe that they need not negotiate for privacy protections."[121]

As a result of the dominant focus on consumer-side market failures, scholars in this camp have thus far offered largely consumer-side solutions to the corporate privacy problem, whether market-based (more common in the United States), or government interventionist (more prominent in Europe). The American market-based consumer solutions typically center on technological consumer self-help efforts called Privacy Enhancing Technology ("PETs").[122] For example, Lawrence Lessig advocates the use of computer software as an "electronic butler" to negotiate privacy preferences.[123] The user would set preferences at the beginning explaining what privacy tradeoffs are permissible, and henceforth the software would negotiate the privacy tradeoffs on behalf of the consumer.[124] Government interventionist proposals have taken a variety of consumer-centric forms, including do-not track lists following the model of the do-not-call list that would allow consumers more control over their privacy.[125]

Although both categories of scholarly explanations for the corporate treatment of privacy offer very different approaches and disparate normative and descriptive conclusions, both camps share a demand-side account of the corporate privacy behavior, as well as demand-side solutions to the problem.[126] The demand-side explanations undoubtedly play an important role in understanding corporate treatment of privacy. This Article, however, seeks to

---

[120] *Id.* at 1452 (quoting Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1398 (2000)).

[121] Chris Jay Hoofnagle & Jennifer M. Urban, *Alan Westin's Privacy Homo Economicus*, 49 WAKE FOREST L. REV. 261, 305 (2014).

[122] *See, e.g.*, LAWRENCE LESSIG, CODE: VERSION 2.0, at 224–27 (2006) (discussing PETs).

[123] LESSIG, *supra* note 113, at 160 ("No one has the time or patience to read through cumbersome documents describing obscure rules for controlling data. What is needed is a way for the machine to negotiate our privacy concerns for us.").

[124] *Id.*

[125] *See generally* Katy Bachman, *Do Not Track Legislation Makes a Comeback*, ADWEEK (Apr. 8, 2013, 10:07 PM), http://www.adweek.com/news/advertising-branding/do-not-track-legislation-makes-comeback-148437 [https://perma.cc/KU4Z-XQQC] (recounting a 2013 proposal, and lobbying efforts against that proposal, in the U.S. Senate to create a nationwide Do Not Track Online registry).

[126] Of course, as with all taxonomies and attempts to categorize, this dichotomy necessarily oversimplifies the far more nuanced and sophisticated arguments of my colleagues. Nonetheless, the overall point that the explanations have largely centered on consumer-side issues with corresponding consumer-side solutions accurately reflects the state of the literature.

explain why such demand-side explanations can be better understood in conjunction with a supply-side story, and how the supply-side story in turn emphasizes the importance of the demand-side failures.

II. Supply-side Corporate Privacy Market Distortion Theory

This Article adds a supply-side corporate privacy market distortion theory to the existing demand-side scholarly accounts seeking to explain why it is that corporations inadequately consider and protect privacy. The overall claim is that a combination of legal and societal structures, including legal corporate disclosure obligations and insatiable and legally unchecked media interest in corporate executives, undermines the ability of those corporate executives to maintain their own personal privacy. This creates a sorting effect by which those individuals who place a high priority or valuation on privacy are less likely to choose to become corporate executives. Consequently, the remaining individuals who do choose to become corporate executives are then less likely to place a high value on their personal privacy because had they prioritized privacy they would have sorted into a different career choice where they could have maintained their privacy. Therefore, the theory predicts that the very same corporate executives tasked with making important corporate decisions that impact privacy are less likely to place a high value on privacy. These low personal privacy preferences on the part of corporate executives then impact the decision making of those executives with regard to corporate privacy issues as the result of a variety of recognized cognitive and behavioral phenomena.

This Part presents the theory as follows. First, it identifies the features of the legal and societal systems that invade the personal privacy of corporate executives.[127] Second, it explores the existing research supporting the view that individual privacy preferences are heterogeneous.[128] Third, it explains why corporate executives would sort by privacy preferences in light of the existing more general research on sorting where there are heterogeneous preferences.[129] It then explains how this sorting results in a phenomenon by which high-level corporate executives at publicly traded companies are disproportionately likely to be drawn from the portion of the population who do not place a high value on privacy, as the privacy-valuing individuals sort away from these sorts of

---

[127] *See infra* notes 133–193 and accompanying text.

[128] *See* Alan F. Westin, *"Whatever Works": The American Public's Attitudes Toward Regulation and Self-Regulation on Consumer Privacy Issues*, *in* Privacy and Self-Regulation in the Information Age 1F (Nat'l Telecomm. & Info. Admin. 1997), http://www.ntia.doc.gov/page/chapter-1-theory-markets-and-privacy [https://perma.cc/4944-BJXM]; Il-Horn Hann et al., *Overcoming Online Information Privacy Concerns: An Information-Processing Theory Approach*, 24 J. Mgmt. Info. Sys. 13, 16 (2007); *infra* notes 194–220 and accompanying text.

[129] *See infra* notes 221–231 and accompanying text.

high-level corporate positions.[130] Finally, it explores the various cognitive and behavioral biases as well as corporate decision-making processes that together help explain how these executives' personal privacy preferences may impact corporate behavior.[131] This occurs, in part, because executives undervalue or potentially do not even recognize the privacy implications of their decisions.[132]

To be clear, this supply-side theory is not intended to provide a stand-alone substitute for the existing demand-side theories. Rather, the supply-side theory offered here, and the existing demand-side theories in the literature, should be viewed as mutually reinforcing explanations that together do a better job of explaining corporate privacy behavior than either theory standing alone. Put differently, if the demand-side privacy market was working well then the supply-side corporate privacy market distortions would not have a significant impact. Conversely, however, the supply-side corporate market distortion helps explain the short-term corporate privacy failures that occur even where the consumer-side market ultimately works fairly well. That is it helps explain the repeated observations in which a corporation has been required to reverse an existing plan or policy with the waste of resources that accompanies such a course reversal as the result of a seemingly unforeseen privacy backlash.

A. Systemic Features Impede Corporate Executive Privacy

Under existing laws and societal practices in the United States, high-level corporate executives working for publicly traded companies are usually unable to keep their personal information private. First, driven partially by the rise in widespread public participation in investments in publicly traded corporations, the media treats corporate executives as public figures whose personal lives are subject to media exposure. Furthermore, courts have not placed any serious limits on the media's ability to invade the privacy of corporate executives as the result of broad interpretations of the public figure and the newsworthiness doctrines with the reduced protection of privacy that goes along with those doctrinal characterizations. Second, a failure to consider privacy within the securities disclosure regime means that large categories of personal facts about corporate executives may be subject to mandatory shareholder disclosure. These features prevent those individuals considering a position as a high-level corporate executive at a publicly traded corporation from being able to trust that they would be able to maintain their personal privacy.

---

[130] *See infra* notes 221–231 and accompanying text.
[131] *See infra* notes 232–255 and accompanying text.
[132] *See infra* notes 232–255 and accompanying text.

1. Corporate Executives Are Treated as Public Figures

The American media has come to treat corporate executives of publicly traded corporations as celebrities worthy of media attention including reporting on various aspects of their personal lives. The resulting loss of privacy is largely driven by two simultaneous societal trends: (1) a growth of the investor pool across a wider cross-section of society and (2) the explosion of information technology.[133]

The United States has seen a large growth in the number of individuals investing directly or indirectly in the stock market. The number of households owning equities in the United States has rapidly expanded from 15.9 million in 1983, to 40 million in 1995, and 56.9 million in 2005.[134] On a percent basis, this increase translates to a change from 19% of American households owning equities in 1983 to 50.3% owning equities in 2005.[135] At the individual level a similar explosion in investment has occurred with the 42.4 million individual U.S. investors owning equities in 1983 ballooning into 91.1 million individual U.S investors, or approximately 1 in 3, owning equities in 2005.[136] This growth in individual investors has been accompanied by an expansion in the pool of individual investors from what used to be mostly wealthy and sophisticated individuals to individuals from all paths of life.[137]

These individual investors, rightly or wrongly,[138] came to view corporate executives as "doppelgangers of their firms," and therefore a primary factor in their investment decision making.[139] This view of the corporate executive led to a demand for a wide variety of information, including personal information about the corporate executive, perhaps because this is the sort of information that the individual investor could digest better than the technical information about a corporation's financial positions.[140]

---

[133] *See* Tom C.W. Lin, *Executive Trade Secrets*, 87 NOTRE DAME L. REV. 911, 923–24 (2012) (noting that the rise of these "two macroeconomic trends has resulted in . . . a depreciation of their individual privacy").

[134] *See* INV. CO. INST. & THE SEC. INDUSTRY ASS'N, EQUITY OWNERSHIP IN AMERICA, 2005, at 1 fig.1 (2005).

[135] *See id.* at 7 fig.9.

[136] *See id.* at 8 fig.10.

[137] *See id.* at 4–5 figs.5 & 7 (showing that investors vary across both age and education).

[138] *See* Marcel Kahan & Edward Rock, *Embattled CEOs*, 88 TEX. L. REV. 987, 989 (2010) (arguing that in recent years CEOs of publicly held corporations are losing power relative to the boards of directors and their shareholders).

[139] Lin, *supra* note 133, at 924–25 (explaining that executives are perceived by investors "not as temporary stewards of business enterprises, but as saviors of industry, alter-egos of firms, and celebrities of society").

[140] *See* Patricia Sánchez Abril & Ann M. Olazábal, *The Celebrity CEO: Corporate Disclosure at the Intersection of Privacy and Securities Law*, 46 HOUS. L. REV. 1545, 1551 (2010) (explaining that "higher investment by average folks" has led to the celebrity status of corporate executives).

In turn, this increased demand in information about corporate executives is happily provided by a media experiencing a simultaneous explosion in information technology. Modern society's expanding use of social media,[141] as well as other technological advances, has created an environment in which the media is able to report on the personal lives of corporate executives.[142] CEOs at many major corporations have received so much media attention, in fact, that Harvard Business School and Sociology Professor Rakesh Khurana dubbed this phenomenon the "distinctly American cult of the CEO."[143] Patricia Sánchez Abril has extensively documented this phenomenon finding that "[o]ver the past half-century, digital communications, globalization, mass-market media and advertising, and a heightened public interest in business matters have conspired to shine a brighter spotlight on business leaders as stars."[144]

Recent news stories provide a multitude of examples demonstrating the increased appetite for and feeding of that appetite with information regarding the personal lives of corporate executives. Consider, for example, Steve Jobs, the well-known founder of Apple Computers. Following Jobs's death in 2011, Americans became so interested in Jobs's life that a biography released soon after his death sold over 379,000 copies in its first week, making it the top selling book in the nation.[145] A later-released film documenting the founder's life raised over $16 million, and was even criticized for not revealing enough about Jobs's personal affairs.[146]

Although Jobs provides an unusual example of just how interested the public can become in the private lives of CEOs and other corporate executives, he is by no means the only corporate figure whose personal life has attracted such high levels of public attention. The CEO of Amazon, Jeff Bezos, provides another good example; as Amazon has continued to grow, so has Bezos's

---

[141] *See, e.g.*, Chris Perry, *Research: Social Media Finally Seen as Essential for CEOs*, FORBES (May 29, 2013, 11:00 AM), http://www.forbes.com/sites/chrisperry/2013/05/29/research-social-media-finally-seen-as-essential-for-ceos/ [https://web.archive.org/web/20160620061302/http://www.forbes.com/sites/chrisperry/2013/05/29/research-social-media-finally-seen-as-essential-for-ceos/#73762ed77126] (noting that 76% of global executives surveyed stated that they wanted the CEOs to be more heavily involved in social media and public engagement).

[142] *See* Lin, *supra* note 133, at 926.

[143] RAKESH KHURANA, SEARCHING FOR A CORPORATE SAVIOR: THE IRRATIONAL QUEST FOR CHARISMATIC CEOS 68 (2002).

[144] Patricia Sánchez Abril, *The Evolution of Business Celebrity in American Law and Society*, 48 AM. BUS. L.J. 177, 178 (2011).

[145] Brandon Griggs, *Steve Jobs Biography Is Top Selling Book in the U.S.*, CNN (Nov. 3, 2011, 10:40 AM), http://www.cnn.com/2011/11/03/tech/innovation/steve-jobs-book-sales/ [http://www.cnn.com/2011/11/03/tech/innovation/steve-jobs-book-sales/].

[146] *Jobs (2013)*, IMDb, http://www.imdb.com/title/tt2357129/ [https://perma.cc/4CV9-Y7JF] (reporting Jobs grossed $16,117,443 in the United States).

public presence.[147] Another prominent corporate figure, Apple's current CEO Tim Cook, has also attracted extensive media attention. Cook appears in the news regularly, and even went so far as to appear on the popular "Late Show with Stephen Colbert" to discuss numerous details of his professional and personal life, including his highly-publicized decision to come out publicly as gay.[148] Warren Buffett, the well-known CEO of Berkshire Hathaway, has also been the focus of public interest for his personal romantic relationships, with articles and even a published biography discussing intimate details about the women in his life.[149]

Although the cult of celebrity surrounding the American CEO is a large part of the phenomenon, Abril found that the business fame also "trickled down to" more ordinary, "rank-and-file executives."[150] The business literature has also extensively documented this "business celebrity culture," as well as the role played by business journalists who reduce complex business dynamics to a corporate executive driven process.[151]

The extensive media and public interest in the private lives of corporate executives has been exacerbated by limited legal protection for the privacy of those corporate executives. In the defamation context, the Supreme Court has held that the First Amendment requires that in order to prevail, individuals found to be public figures must prove that the defamatory statement was made with "actual malice."[152] This means that the defendant must have had actual knowledge that the statement was false, or acted with reckless disregard as to whether it was false or not.[153] Furthermore, the actual malice requirement must be proved by clear and convincing evidence.[154] Establishing actual malice in

---

[147] Tim Appelo, *10 Things You Didn't Know About Jeff Bezos and Amazon*, HOLLYWOOD REP. (Oct. 18, 2013, 2:58 PM), http://www.hollywoodreporter.com/news/10-things-you-didnt-know-649386 [https://perma.cc/8RN8-VZSW] (discussing the publication of an extensive book about Bezos and his life, based on stories from over 300 sources).

[148] Keith Wagstaff, *Apple CEO Tim Cook Talks Steve Jobs with Stephen Colbert*, NBC NEWS (Sept. 16, 2015, 11:13 AM), http://www.nbcnews.com/tech/tech-news/apple-ceo-tim-cook-talks-steve-jobs-stephen-colbert-n428316 [https://perma.cc/47XV-TMAG].

[149] Barbara Kiviat, *Warren Buffet Tells All: The Women in His Life*, TIME (Sept. 23, 2008), http://content.time.com/time/business/article/0,8599,1843839,00.html [https://perma.cc/GS3M-9YV4].

[150] Abril, *supra* note 144, at 178.

[151] *Id.* at 179 (citing Mathew L.A. Hayward et al., *Believing One's Own Press: The Causes and Consequences of CEO Celebrity*, 25 STRATEGIC MGMT. J. 637, 645 (2004)).

[152] N.Y. Times Co. v. Sullivan, 376 U.S. 254, 279–80 (1964); *see also* Laura A. Heymann, *The Law of Reputation and the Interest of the Audience*, 52 B.C. L. REV. 1341, 1379–80 (2011) (explaining further the "actual malice" standard enunciated in the Court's holding in *New York Times Co. v. Sullivan*).

[153] *See N.Y. Times Co.*, 376 U.S. at 279–80.

[154] Gertz v. Robert Welch, Inc., 418 U.S. 323, 342 (1974); *see also* David Han, *Rethinking Speech-Tort Remedies*, 2014 WIS. L. REV. 1135, 1184 (discussing the various rules governing public figures).

defamation cases has proved extremely challenging, such that receiving public figure status makes winning a defamation lawsuit a long shot.[155]

Abril's work demonstrates that "major cases analyzing whether business executives are public figures map neatly onto the historical rise of business celebrity culture."[156] In early cases, businessmen were typically found to be private figures, but as business gained notoriety in the 1980s, they "morphed into public figures in the eyes of the law."[157] By the 1990s, Abril discovered a notable absence of defamation cases involving corporate executives.[158] She persuasively hypothesizes that this collapse in cases is best explained by recognition on the part of the corporate executives that their notoriety spelled defeat for any possible defamation lawsuit, rather than an actual reduction in defamatory invasions of their privacy.[159] Consequently, she concludes that "[p]ublic notoriety became part of the job description of some CEOs with diminished privacy being an occupational hazard."[160]

Because probable public figure status means that corporate executives find it extremely difficult to keep defamatory statements about themselves out of the press, predictably under the existing legal frameworks, they will find it even more impossible to keep truthful, but personal information private. Under the public disclosure of private facts tort, individuals can sue to prevent the dissemination of private facts about them that would be highly offensive and objectionable to a reasonable person.[161] Much private personal information about the corporate executive including his or her lifestyle choices, divorce, and health conditions may not be considered shameful enough to meet the

---

[155] *See* St. Amant v. Thompson, 390 U.S. 727, 731 (1968) (finding that petitioner did not act with actual malice when falsely accusing a public official of engaging in criminal conduct); Tavoulareas v. Piro, 817 F.2d 762, 775–76 (D.C. Cir. 1987) ("It is equally well established that the standard of actual malice requires proof not merely that the defamatory publication was false, but that the defendant either knew the statement to be false or that the defendant in fact entertained serious doubts as to the truth of his publication."); *see also* David A. Anderson, *Is Libel Law Worth Reforming?*, 140 U. PA. L. REV. 487, 493 (1991) (explaining the difficulty of proving actual malice).

[156] Abril, *supra* note 144, at 183.

[157] *Id.*

[158] *Id.* at 203–04.

[159] *Id.* at 204.

[160] *Id.*; *see also* Scott J. Shackelford, *Fragile Merchandise: A Comparative Analysis of the Privacy Rights for Public Figures*, 49 AM. BUS. L.J. 125, 145 (2012) (stating that corporate executives "fall into the voluntary public figure category and hold almost as limited a claim to a right of privacy as do public officials").

[161] *See* RESTATEMENT (SECOND) OF TORTS § 652D (AM. LAW INST. 1977); *see also* Doe v. Gangland Prods., 730 F.3d 946, 958–59 (9th Cir. 2013) (explaining the requirements for proving a claim for public disclosure of private facts); Shulman v. Grp. W Prods., Inc., 955 P.2d 469, 478 (Cal. 1998) (analyzing the elements of the publication of private facts tort).

offensiveness requirement of the tort.[162] Even if the corporate executive could meet that offensiveness hurdle, however, the tort contains an absolute defense for information that is considered "of legitimate public concern," which has been interpreted by some courts as a finding of "newsworthiness."[163] Newsworthiness appears to be an even lower standard than the public figure test in the defamation context,[164] and is often met as long as there is public interest in the matter.[165] The newsworthiness test, in today's society, appears to be met for all information related to corporate executives. Therefore, corporate executives can hope for very little protection from either defamation law or the relevant privacy torts to keep their information private from inquiring business media and its hungry audience.[166]

---

[162] *See, e.g.*, Taus v. Loftus, 151 P.3d 1185, 1207 (Cal. 2007) (expressing doubt whether a statement that the plaintiff had engaged in unspecified "destructive behavior" would satisfy the offensiveness requirement because it was an insufficiently "sensitive or intimate private fact").

[163] *See Shulman*, 955 P.2d at 478 (concluding that the "analysis of newsworthiness inevitably involves accommodating conflicting interests in personal privacy and in press freedom as guaranteed by the First Amendment to the United States Constitution"). The court stated that

> where the facts disclosed about a private person involuntarily caught up in events of public interest bear a logical relationship to the newsworthy subject of the broadcast and are not intrusive in great disproportion to their relevance—the broadcast was of legitimate public concern, barring liability under the private facts tort.

Id.

[164] *See* Haynes v. Alfred A. Knopf, Inc., 8 F.3d 1222, 1232 (7th Cir. 1993) (explaining in analyzing a public disclosure of private facts tort that "[p]eople who do not desire the limelight and do not deliberately choose a way of life or course of conduct calculated to thrust them into it nevertheless have no legal right to extinguish it if the experiences that have befallen them are newsworthy, even if they would prefer that those experiences be kept private").

[165] *See* Wolston v. Reader's Digest Ass'n, 443 U.S. 157, 167–68 (1979) (suggesting that newsworthiness equates public interest by stating in a defamation case that plaintiffs actions "no doubt were 'newsworthy,' but the simple fact that these events attracted media attention also is not conclusive of the public-figure issue," and that "[a] private individual is not automatically transformed into a public figure just by becoming involved in or associated with a matter that attracts public attention").

[166] *See* Abril & Olazábal, *supra* note 140, at 1581 (finding that "strong arguments can be made that any information bearing on the honesty, integrity, or ability of the head of a publicly traded corporation is legitimately newsworthy" and therefore corporate executives "enjoy an extremely limited private sphere"); Tom C.W. Lin, *Undressing the CEO: Disclosing Private, Material Matters of Public Company Executives*, 11 U. PA. J. BUS. L. 383, 424 (2009) (arguing that corporate executives "should reasonably expect to abdicate a certain level of privacy" as "[t]he proliferation of new media coupled with the growth in securities investing by ordinary citizens has further intensified coverage of public company executives" and fed "the public's insatiable appetite for more information"); *cf.* Lior Jacob Strahilevitz, *Toward a Positive Theory of Privacy Law*, 126 HARV. L. REV. 2010, 2014 (2013) (explaining that "privacy protections for people voluntarily in the public eye in the United States are basically negligible").

2. Corporate Disclosure Requirements Invade Privacy

As explained above, corporate executives are already forced to give up their personal privacy as the result of the intense scrutiny by the media and the public. For executives of publicly traded corporations, this loss of privacy is exacerbated by an unintended consequence of an ambiguous securities law corporate disclosure regime that was understandably designed without any consideration of the privacy impact on corporate executives.[167]

First, corporate disclosure rules mandate disclosing certain categories of personal information about corporate executives including the executive's age,[168] involvement in certain legal proceedings including personal bankruptcy filings,[169] and the compensation packages for five highly paid executives.[170] More significantly, other personal information about corporate executives can potentially fall under the catchall disclosure regime created by the Exchange Act and SEC rules, which requires disclosing material information, where a duty to disclose arises.[171] Under governing Supreme Court precedent, factual information about a corporation becomes material if there exists a substantial likelihood that a reasonable shareholder would consider the factual information important in making an investment decision, or if a reasonable investor would view disclosure of the fact as significantly altering the "total mix" of

---

[167] *See generally* Victoria Schwartz, *Disclosing Corporate Disclosure Policies*, 40 FLA. ST. U.L. REV. 487, 505–07 (2013) (discussing problems with the securities law corporate disclosure regime).

[168] 17 C.F.R. § 229.401(b) (2016). Item 401 of Regulation S-K requires disclosure of general biographical detail including the executive's age. *Id.*

[169] *Id.* § 229.401(f)(1)–(2). Item 401(f) of Regulation S-K requires the company to disclose the CEO's personal bankruptcy filings, any adjudicated violations of the securities or commodities laws, and whether the executive "was convicted in a criminal proceeding or is a named subject of a pending criminal proceeding (excluding traffic violations and other minor offenses)." *Id.* On its face, this rule does not apply to most types of civil litigation, such as divorce or a criminal investigation that did not result in a criminal proceeding. *Id.*

[170] *Id.* § 229.402. Regulation S-K, Item 402, requires disclosure of the salary, bonus, stock awards, stock option awards, and other compensation elements for the principle executive officer, principal financial officer, and the other three most highly compensated executive officers. *Id.*

[171] *See* 15 U.S.C. § 78j(b) (2012); *see also* 17 C.F.R. § 240.10b-5(b) (2015). Scholars and practitioners disagree as to whether there is anything in the securities laws that creates a duty to disclose personal information about executives. *Compare* Abril & Olazábal, *supra* note 140, at 1591 (finding no basis for an affirmative duty to disclose private CEO facts), *with* Allan Horwich, *When the Corporate Luminary Becomes Seriously Ill: When Is a Corporation Obligated to Disclose That Illness and Should the Securities and Exchange Commission Adopt a Rule Requiring Disclosure?*, 5 N.Y.U. J.L. & BUS. 827, 838 (2009) (finding "little doubt" that the existing disclosure requirements "would encompass material uncertainties arising out of a known health problem suffered by a luminary"), *and* Joan MacLeod Heminway, *Personal Facts About Executive Officers: A Proposal for Tailored Disclosures to Encourage Reasonable Investor Behavior*, 42 WAKE FOREST L. REV. 749, 790, 802 (2007) (explaining the difficulty in determining SEC disclosure requirements and proposing "relatively straightforward mandatory disclosure rules").

information.[172] So-called "soft information" about a corporation—generally predictions and other forward-looking information—becomes material based on a different test that involves the "balancing of both the indicated probability that the event will occur and the anticipated magnitude of the event in light of the totality of the company activity."[173]

These two tests presumably apply to determine whether the corporation is required to disclose personal information about corporate executives to its shareholders. Significantly, there is no privacy exception to the corporation's disclosure requirements. In fact, neither of these tests takes into account any consideration of the corporate executive's privacy interest as a countervailing consideration weighing against disclosure.[174]

Therefore, if there is either a substantial likelihood that a reasonable shareholder would consider the information important in making an investment decision, or view the disclosure of the information as significantly altering the "total mix" of information, then corporate executives' personal information may be subject to disclosure. Various personal facts about corporate executives may satisfy this test including health information, financial trouble, divorce, extramarital affairs or other romantic liaisons, the purchase of homes or other large luxury items, and the death or illness of a child or other loved one.[175] Shareholders might legitimately consider some personal information about executives relevant because it provides insight into the ability of the executive to do his or her job. This may result from concern about the executive's ability to adequately focus on the job, or alternatively because there is concern as to whether the executive will stay on the job.

In the first scenario where there is concern about an executive's ability to focus on the job, the disclosure of the personal fact signals to the shareholder that the executive's effectiveness on the job is impaired because the personal fact represents some sort of distraction or other impediment to the executive's typical time, energy, or focus on the company.[176] Various personal facts about the executive might trigger this concern about his or her ability to perform the job including the distraction that results from going through a messy divorce, or the challenges that result from the death of a family member. The limited

---

[172] Basic Inc. v. Levinson, 485 U.S. 224, 231–32 (1988) (quoting TSC Indus., Inc. v. Northway, Inc., 426 U.S. 438, 449 (1976)).

[173] *Id.* at 238.

[174] *See* Schwartz, *supra* note 167, at 507.

[175] *See id.* at 494–97.

[176] Some scholars have downplayed the legitimacy of the disclosure interest in personal information about executives as merely an example of celebrity-fascination. Although celebrity fascination is certainly part of the picture, this Article offers an account of disclosure in which there are legitimate reasons beyond celebrity fascination for why shareholders and investors would care about the information.

empirical research that exists supports this shareholder concern. Finance scholars at NYU's Stern School of Business found that the profitability of a company on average diminished by approximately 2.4 percentage points in the two years following the death of a CEO's child as compared to the previous two years.[177] The scholars reported a similar drop in the company's return on assets following the death of a CEO's parent (although no change following the death of a mother-in-law).[178] This suggests there is a substantial likelihood that a reasonable shareholder would consider the deeply personal information about a death in the executive's family to be relevant in making an investment decision.

In the second scenario where there is concern as to whether an executive will stay on the job, shareholders would consider personal information relevant to their investment decisions if the information provides insight regarding the executive's ability to retain the job. This may matter to shareholders because they believe a particular executive is unusually good at his or her job, and there is a concern that the successor may not be equally effective. Alternatively, this may matter to the shareholders because of a belief that the company is not well situated to go through a smooth leadership transition. Of course this transition concern could be ameliorated with better succession planning, but nonetheless this remains a legitimate concern for shareholders.[179] Finally, shareholders may believe that a particular executive is underperforming, but that due to capture and other corporate governance issues the board is unlikely to remove him or her. In that scenario, shareholders might consider personal information that suggests that the executive is likely to leave as a positive input impacting the investment decision. Personal facts that could impact the executive's ability to stay on the job include a serious or terminal illness or serious criminal legal problems. The limited empirical research supports this shareholder concern with losing an executive as well.[180]

These scenarios suggest that a wide variety of personal information about executives—including such private sensitive information as health information and challenges with an individual's family—could fit into the definitions of materiality. And as stated earlier, the rules do not contain any exception that would permit the executive's privacy to outweigh the disclosure requirement.

---

[177] Morten Bennedsen et al., Do CEO's Matter? 15 (Dec. 2010) (unpublished manuscript), available at https://www0.gsb.columbia.edu/mygsb/faculty/research/pubfiles/3177/valueceos.pdf [https://perma.cc/58FP-FTDA] (using data from Denmark).

[178] *Id.*

[179] *See, e.g.*, Lin, *supra* note 133, at 945–46 (pointing out the importance of succession plans to a company's stability and success).

[180] *See* Jesus M. Salas, *Entrenchment, Governance, and the Stock Price Reaction to Sudden Executive Deaths*, 34 J. BANKING & FIN. 656, 657 (2010) (reviewing the literature that has found negative reactions to sudden executive deaths).

Predictably, actual corporate disclosure behavior mimics the ambiguity in the existing securities disclosure regime regarding whether and when personal information about executives must be disclosed to shareholders. On one hand, Apple took a strong non-disclosure position with regard to the health of Steve Jobs, choosing to remain silent in the face of Jobs's early fight with cancer, and continuing to make vague statements as his health declined.[181] Numerous other companies have similarly disclosed very little.[182] On the other hand, Berkshire Hathaway took a different approach to the health of Warren Buffett, choosing to provide a detailed press release to shareholders providing details of Buffett's colon surgery.[183] Other companies have also chosen to disclose information about its executives based on an apparent belief that it is legally required for them to do so.[184] Legally and practically, at best there is confusion regarding whether corporations must disclose information about corporate executives to their shareholders, resulting in an inability of corporate executives to trust that they will be able to protect their privacy should they desire to do so. As such, the corporate disclosure requirements thus act as a sort of tax, or a legal wedge that distorts the labor market for corporate executives.

3. Other Privacy Laws Fail to Fill in the Gap

The various federal and state statutory privacy laws do not adequately protect the privacy of the corporate executive (or anyone else for that matter), because they are specifically tailored to particular scenarios or contexts.[185] For example, although HIPAA governs the privacy of health information,[186] it only applies to "covered entities," which does not include either the media or the corporate employer.[187] Similarly, the Right to Financial Privacy Act of 1978 only applies to banks or other financial institutions, and would not govern the media or corporate employer.[188] Furthermore, the Right to Financial Privacy

---

[181] *See* Schwartz, *supra* note 167, at 512–14 (documenting the saga involving Apple's failure to disclose Jobs's deteriorating health condition).

[182] *See id.* at 515 (noting that both Intel and Bear Stearns elected to hide the prostate health issues of their CEOs).

[183] *Id.* at 514.

[184] *Id.* (documenting the General Motors vice-chairman as opining that "there is an absolute requirement to make full disclosure").

[185] *See* Abril & Olazábal, *supra* note 140, at 1567–75 (explaining that many privacy statutes apply in very limited circumstances and have "idiosyncratic application").

[186] Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (codified as amended in scattered sections of 18, 26, 29 and 42 U.S.C.).

[187] *See* 45 C.F.R. § 160.103 (2015) (defining covered entities as health plans, health care clearinghouses, health care providers, and business associates to those covered entities).

[188] Right to Financial Privacy Act of 1978, 12 U.S.C. §§ 3401–3422 (2012) (defining "financial institution" as "any office of a bank, savings bank, card issuer . . . industrial loan company, trust

Act of 1978 protects the confidentiality of customers' financial information, not the financial records of executives or other employees.[189]

Some privacy-related statutes do apply to the corporation as an employer, but only limit the use of information obtained in very specific scenarios. For example, the Americans with Disabilities Act, the Rehabilitation Act, and the Family and Medical Leave Act all contain nondisclosure provisions.[190] The case law interpreting these statutes, however, has limited those provisions to information obtained as the result of an authorized medical examination or inquiry, and has excluded information obtained by voluntary disclosure by the employee, which has been interpreted quite broadly.[191] Similarly, the Employee Polygraph Protection Act of 1988 limits protections to information obtained as the result of a prohibited lie detector test.[192] Additionally, the Fair Credit Reporting Act only covers an employer's use of information collected as part of a "consumer report" on the employment application.[193]

In summary, the combination of: (1) the diversification of the investor pool resulting in increased media and public interest in corporate executives, (2) the boom in information technology resulting in widespread reporting on such corporate executives, (3) the lack of legal protection for the private lives of the corporate executives, and (4) the ambiguity regarding whether corporations are required to disclose private facts about corporate executives to their shareholders, all combine to result in a system in which candidates looking to become corporate executives at publicly traded companies cannot trust that they will be able to maintain their privacy.

---

company, savings association, building and loan, or homestead association (including cooperative banks), credit union, or consumer finance institution").

[189] *See id.* § 3403 (stating that "[a] financial institution shall not release the financial records of a *customer*" unless it is a permissible disclosure under the statute) (emphasis added).

[190] *See* Rehabilitation Act of 1973 § 504, 29 U.S.C. § 794 (2012); Family and Medical Leave Act of 1993, 29 U.S.C. §§ 2601–2654 (2012); Americans with Disabilities Act of 1990 ("ADA"), 42 U.S.C. §§ 12101–12213 (2012). Congress has provided that ADA standards shall also apply to the Rehabilitation Act. *See* 29 U.S.C. § 791(f) (2012). ADA regulations, which apply to federal employees under the Rehabilitation Act, make information obtained under the act by employers confidential and limits disclosure. *See* 29 C.F.R. § 1630.14 (2015).

[191] *See* Schwartz, *supra* note 167, at 510–11 (discussing cases interpreting these statutes).

[192] 29 U.S.C. § 2008 (stating that neither the polygraph examiner nor the employer for whom the test is conducted may disclose information obtained during the test except in limited circumstances).

[193] 15 U.S.C. §§ 1681a–1681b (2012) (allowing a consumer reporting agency to furnish a report to a person that intends to use the information for "employment purposes" and defining "employment purposes" as having the "purpose of evaluating a consumer for employment, promotion, reassignment or retention as an employee").

B. Heterogeneity in Individual Privacy Preferences

The inability of corporate executives to maintain their privacy would not have a significant sorting effect if privacy preferences were homogenous. The existing evidence suggests, however, that individual privacy preferences, like many types of preferences, are heterogeneous, meaning that some individuals inherently have more of a taste for privacy than others.[194] Although most of the existing experimental and survey research-based empirical work has been done within the consumer context, nothing about the studies or underlying theory suggests that consumers have unique characteristics such that the conclusions about heterogeneity of privacy preferences cannot be inferred from a consumer population to the population at large more generally.

Prominent privacy scholar Alan Westin extrapolated from decades of privacy opinion surveys to conclude that the American public can be divided into three categories of privacy preferences.[195] At one extreme are individuals that Westin titled the "privacy fundamentalists," which Westin estimated comprised approximately twenty-five percent of the population.[196] Consistent with their name, privacy fundamentalists view privacy as extremely high value and are largely unwilling to trade away their privacy.[197] Privacy fundamentalists reject the suggestion that business and governmental programs are entitled to receive personal information, and believe that more individuals should refuse to give out requested information.[198]

Westin named the middle and largest category of individuals, estimated at fifty-five percent of the population, the "privacy pragmatists."[199] This group takes a more nuanced approach to privacy, in which any requests for personal information get balanced against the benefits from disclosing the requested information.[200] Privacy pragmatists often base their decision on the degree of trust in the particular industry or company involved.[201]

Finally, the least privacy concerned group, which Westin dubbed "privacy unconcerned" and estimated at twenty percent of the population, does not have any objection to supplying personal information to either the government or

---

[194] S*ee* Schwartz, *supra* note 167, at 502–05.

[195] *See* Westin, *supra* note 128, at 1F; *see also Opinion Surveys: What Consumers Have to Say About Information Privacy: Hearing Before the Subcomm. on Commerce, Trade and Consumer Protection of the Comm. on Energy and Commerce*, 107th Cong. 18 (2001) (statement of Alan Westin, Professor Emeritus, Columbia University).

[196] Westin, *supra* note 128, at 1F.

[197] *Id.*

[198] *Id.*

[199] *Id.*

[200] *Id.*

[201] *Id.*

businesses.[202] Westin found that not only did the privacy unconcerned have no problem giving up their own information, but they entirely failed to recognize what the privacy fuss is all about.[203] This failure by the privacy unconcerned to even understand what the privacy fuss is all about will become important later in this Section, in discussing the implications of the sorting effect by corporate leadership.

Although Westin's methodologies and the breakdown of his categories have been questioned by scholars, none of these criticisms have attacked or even questioned the core conclusion that individual privacy preferences are heterogeneous.[204] On the contrary, other scholars have been able to replicate Westin's categories of heterogeneous privacy preferences in different contexts using similar survey methodologies, although they found slight differences in the exact breakdowns of the categories.

For example, in a survey studying the online privacy concerns of Internet users, computer scientist Mark S. Ackerman and his team found that 17% of respondents were privacy fundamentalists who were extremely concerned about any use of their data, and were unwilling to provide data to websites even with privacy protections in place.[205] Fifty-six percent of respondents comprised the pragmatic majority whose privacy concerns were often significantly reduced by the presence of privacy protection measures.[206] Finally, 27% of respondents, renamed the "marginally concerned," were willing to provide data to websites under almost any condition.[207]

Subsequently, an additional study by information systems scholars Sarah Spiekermann, Jens Grossklags, and Bettina Berendt also found heterogeneity of privacy preferences.[208] This study revealed a slightly higher percentage of privacy fundamentalists at 30%, and a slightly lower percentage of marginally concerned at 24%, than the Ackerman study.[209] Furthermore, the study broke down the pragmatic majority that had been identified by Westin and confirmed

---

[202] *Id.*

[203] *Id.*

[204] *See* Stephen T. Margulis, *On the Status and Contribution of Westin's and Altman's Theories of Privacy*, 59 J. SOC. ISSUES 411, 411–29 (2003) (critiquing Westin and Altman's theories of privacy and summarizing the theory and research that have been a consequence of their theories). *See generally* Hoofnagle & Urban, *supra* note 121, at 261 (challenging "Westin's assumptions in categorizing consumers" into the various segments as well as Westin's depiction of the way that privacy pragmatists are supposed to behave).

[205] Mark S. Ackerman et al., *Privacy in E-Commerce: Examining User Scenarios and Privacy Preferences*, PROC. IN THE ACM CONF. ON ELECTRONIC COM. 1, 3 (1999).

[206] *Id.*

[207] *Id.*

[208] Sarah Spiekermann et al., *E-Privacy in 2nd Generation E-Commerce: Privacy Preferences Versus Actual Behavior*, PROC. OF THE 3RD ACM CONF. ON ELECTRONIC COM. 38, 42 (2001).

[209] *Id.*

by Ackerman into two distinct groups.[210] The "identity concerned" group, comprising 20% of the full sample, encompassed individuals whose privacy concerns focused on the revelation of identity aspects such as name, address, or e-mail.[211] The "profiling adverse" group, comprising 26% of the overall surveyed population, primarily focused on the profiling of interests, hobbies, health, and other personal information.[212]

Heterogeneity in privacy preferences has also been found using other non-survey based methodologies. For example, business scholar Il-Horn Hann, and information systems scholars Kai-Lung Hui, Tom S. Lee, and I.P.L. Png also found strong support for their privacy diversity hypothesis that individuals have systematic differences in privacy preferences.[213] They too identified three distinct segments in the studied population with very different attitudes toward privacy.[214] Rather than Westin's methodological choice of opinion surveys, these scholars first used conjoint analysis, a measurement method for decision-making contexts where multiple dimensions must be considered, across focus groups to assess trade-offs among two benefits and three privacy concerns.[215] Then employing cluster analysis,[216] they found that seventy-two percent of American subjects can be characterized as "privacy guardians"—individuals who attach a relatively high value to information privacy.[217] By contrast, a smaller group of American subjects can be characterized as "information sellers"—those who place very little emphasis on privacy and are thus willing to trade their privacy for a perceived monetary reward.[218] Finally, a third small group, "convenience seekers," focused exclusively on convenience with little regard for money or privacy.[219]

Although the conjoint analysis methodology divided up the privacy categories differently than Westin did, both sets of scholarship are consistent with a conclusion that individual privacy preferences are heterogeneous.

---

[210] *Id.*

[211] *Id.*

[212] *Id.*

[213] Hann et al., *supra* note 128, at 21, 30.

[214] *Id.* at 30, 32.

[215] *Id.* at 21. According to the authors, conjoint analysis is a technique that grew out of the area of conjoint measurement developed in economics and psychology where the researcher presents test subjects with a set of alternatives consisting of particular levels of various dimensions. *Id.* The test subject is then asked to rank the alternatives based on individual preferences. *Id.* Conjoint analysis then assumes that the ranking can be decomposed into the sum of contributions from the various dimensions. *Id.* Then each part-worth is equivalent to the marginal utility of the dimension in the individual's ranking of the conjoint stimuli. *Id.*

[216] Cluster analysis "groups subjects into distinct segments according to the similarity of their estimated coefficients for the various outcomes." *Id.* at 30.

[217] *Id.*

[218] *Id.* at 30–31.

[219] *Id.*

Therefore, regardless of where exactly the lines of categories are drawn, it seems likely that individual privacy preferences range a full spectrum from caring deeply, to caring somewhat, to not caring very much at all. In light of all this evidence, privacy scholars have embraced the conclusion that privacy preferences are heterogeneous.[220]

C. Corporate Executives Sort Away From Privacy

Given the existence of heterogeneous privacy preferences, the next step in the supply-side corporate privacy market distortion theory is to examine the privacy preferences likely held by corporate executives. This subpart identifies some reasons to believe that overall corporate executives fall on the low end of the privacy spectrum, meaning that they do not place a high value on their own privacy as the result of a sorting mechanism.

Employees at all levels engage in sorting.[221] Sorting means that individual employees move across different employment situations and even industries in order to maximize the things they prioritize. The sorting phenomenon relies on the assumption that employees have heterogeneous preferences with regards to various features of employment.[222]

For example, if a group of individuals highly values schedule flexibility, then those individuals likely sort themselves into employment with employers who offer more schedule flexibility. If, however, an entire industry or position does not offer schedule flexibility, then one would expect individuals who highly value schedule flexibility to sort toward another industry or a different

---

[220] *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) (pointing to the plethora of survey and experimental data supporting the heterogeneity of privacy preferences in the context of evaluating privacy protections in the health context); 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*)."); Strahilevitz, *supra* note 166, at 2026 ("American attitudes toward privacy are highly heterogeneous."); Felix T. Wu, *The Constitutionality of Consumer Privacy Regulation*, 2013 U. CHI. LEGAL. F. 69, 75 (noting that notice-and-choice is "normatively attractive 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").

[221] *See* Naomi Schoenbaum, *Mobility Measures*, 2012 B.Y.U. L. REV. 1169, 1177–87 (explaining the various features of employment law that facilitate such sorting).

[222] Sharon Hannes, *Reverse Monitoring: On the Hidden Role of Employee Stock-Based Compensation*, 105 MICH. L. REV. 1421, 1431 (2007) (pointing out that employee stock ownership plans sort among employees who are heterogeneous in their beliefs regarding the firm's prospects in favor of those who are either more optimistic or more risk tolerant).

type of position that maximize as many of those individuals' other priorities as possible, but that also allows for increased schedule flexibility.[223] Individuals who do not place a high value on schedule flexibility, however, will sort based on features that matter more to them such as earning higher wages, developing human capital, or achieving more fulfillment in their work.[224] The flip-side of this phenomenon is that the same features that cause individuals to sort into employment with a particular employer, into a particular industry, or into a particular type of position, can cause others to sort out of those exact same employers, industries, or positions.[225]

By no means is sorting a perfectly efficient phenomenon. The claim is not that every single individual placing a high value on schedule flexibility will sort themselves into a job where they can have schedule flexibility. Individuals need to balance a variety of complex factors, and most employees place a high value on various terms and conditions of employment, and need to figure out how to balance across the options in different job markets. The claim is merely that all else being equal, individuals who place a high value on a particular feature of employment will tend to overall sort themselves into employment containing that employment feature if possible given their other priorities.

The sorting dynamic is not limited to low-level employees. Rather, a similar phenomenon can occur with the category of candidates who might be qualified to become corporate executives, in which features about corporate executive positions will lead individuals with various characteristics to sort themselves into different career choices.[226] For example, scholars have noted the way in which structuring executive compensation as pay for performance with large percentages of stock options can lead to a sorting effect in favor of individuals becoming corporate executives with high tolerances for risk[227] or

---

[223] *See* Forrest Briscoe, *Temporal Flexibility and Careers: The Role of Large-Scale Organizations for Physicians*, 60 INDUS. & LAB. REL. REV. 88, 91 (2006) ("If large-scale organizations offer physicians more schedule and career flexibility, then we should expect a degree of labor market sorting in which physicians who value that flexibility disproportionately choose employment in large-scale settings.").

[224] *See, e.g.*, Peter C. Coyte, *Specific Human Capital and Sorting Mechanisms in Labor Markets*, 51 S. ECON. J. 469, 470–72 (1984) (explaining that things like probationary contracts act as sorting mechanisms by "discouraging applications from those who believe their probability of passing the test is low"); *see also* Schoenbaum, *supra* note 221, at 1177–87 (explaining the various features of employment law that facilitate such sorting).

[225] Jonah Gelbach et al., *Passive Discrimination: When Does It Make Sense to Pay Too Little?*, 76 U. CHI. L. REV. 797, 799 (2009) (pointing out that certain compensation packages will attract certain types of workers, but discourage other individuals from applying for or accepting the job).

[226] *See* Saul Levmore, *Puzzling Stock Options and Compensation Norms*, 149 U. PA. L. REV. 1901, 1928 (2001) (explaining that the sorting of employees based on risk levels occurs for employees at all levels including corporate executives).

[227] *See id.*

high emphasis on monetary rewards and financial metrics as opposed to other goals.[228]

Just like other non-monetary aspects of employment for which employees have heterogeneous preferences, individual employees also sort themselves based on their heterogeneous privacy preferences. Within a particular industry or career, individuals can sort toward privacy protective employers if they have both the choice and information to do so. For example, if some big law firms began to engage in various privacy-invasive behaviors such as GPS tracking, keystroke monitoring, etc., one would expect individuals with higher privacy valuations to sort away from those firms and towards firms who do not engage in those privacy-invasive behaviors. If, however, an entire industry or type of job position necessarily involved an invasion of privacy, then individuals who highly prioritize privacy would be expected to sort away from those industries or jobs. Thus one would expect that individuals who highly value privacy would not pursue appearing on reality television.[229] Similarly, individuals who highly value privacy and are interested in policymaking might be expected to choose to work behind-the-scenes for a politician, but would likely not choose to actually run for political office.[230]

As a consequence of the features of the existing legal system discussed above, candidates capable of becoming high-level executives at publicly traded corporations are unable to trust that they will be able to keep their personal information private. Consequently, consistent with the theory of employee sorting, the market for corporate executives will also be subject to a sorting effect in which highly qualified individuals who strongly value privacy will

---

[228] *See* Tamara C. Belinfanti, *Beyond Economics in Pay for Performance*, 41 HOFSTRA L. REV. 91, 136 (2012) ("[Pay for performance] may unwittingly encourage a kind of selective sorting among potential CEOs. Individuals who are attracted to simply meeting monetary rewards will be attracted to becoming a CEO, while those who resist this type of reductionist view of their work and their ethics may be driven to seek another position.") (alteration in original).

[229] *See* Jennifer L. Carpenter, *Internet Publication: The Case for an Expanded Right of Publicity for Non-Celebrities*, 6 VA. J.L. & TECH. 3, 30 (2001) (noting that "there may be some truth behind the assumption that most celebrities value exposure, whereas non-celebrities value privacy"). That said, it may not be expected that the same type of sorting with regard to such celebrities as musicians and actors to the extent that pursuing a career as a musician or an actor necessarily means subjecting oneself to celebrity. To the extent that someone with a talent or passion for acting or music does not have a good avenue to pursue a career in acting or music without also pursuing celebrity, it may be possible to have actors or musicians who become celebrities but who also value privacy.

[230] I am working on a companion paper arguing that a similar privacy sorting effect with similar decision-making consequences occurs with regard to politicians and helps explain the relative lack of privacy laws in the United States. *Cf.* David H. Flaherty, *Reflections on Reform of the Federal Privacy Act*, 21 CAN. J. ADMIN. L. & PRAC. 271, 316 (2008) (noting in the Canadian context that "[f]ew politicians in power care about privacy, except in a privacy crisis needs to be urgently managed in the usual manner; i.e., fending off the Opposition, the media, and concerned portions of the public. At best, privacy is a generic concern that does not rise to the level of the need for action").

choose to take their talents in different directions and instead will opt for other sorts of careers, which would be less likely to require them to forego their own personal privacy. Even if those privacy-valuing individuals also (like most people) place a high value on money, talented individuals with corporate-executive type resumes usually still have the option to pursue other types of business-oriented careers where they can expect high levels of compensation without foregoing their privacy, such as perhaps working in banking, hedge funds, management consulting, and private equity.[231] As a consequence of this sorting effect, the individuals that remain in pursuit of the high-level corporate executive positions are less likely to be drawn from the population that highly values privacy. Put differently, by failing to adequately protect the privacy of corporate leadership, the existing legal system makes it more likely that the individuals who choose to pursue corporate leadership do not themselves care about privacy.

D. Privacy Sorting Impacts Corporate Privacy Decisions

Corporate executives are in a position to make decisions with tremendous privacy implications for corporate constituents. After all, corporate actors have a great deal of power to shape the treatment of privacy.[232] As explained above, the privacy sorting phenomenon means that individuals who choose to become corporate executives are less likely to place a high value on privacy.

Even if the majority of corporate executives were evenly distributed across the lower-privacy side of the heterogeneous privacy spectrum, that would still mean that a disproportionate number of corporate executives are drawn from the population that Westin called the "privacy unconcerned" as compared with the population as a whole.[233] This is particularly concerning in light of Westin's findings that individuals who are privacy unconcerned not only do not care about their own privacy, but actually don't understand what the entire privacy fuss is all about.[234] This suggests that a disproportionate number of corporate executives not only don't care about their own privacy, but also actually fail to even recognize why others might be concerned about their privacy. Perhaps with this perspective in mind, McNealy's oft-repeated statement that individuals "have zero privacy anyway" and should just "get

---

[231] *See* Brian Cheffins & John Armour, *The Eclipse of Private Equity*, 33 DEL. J. CORP. L. 1, 59 (2008) (noting that "[p]rivacy has been an integral element of the private equity industry" which is not subject to traditional disclosure regulations); Steven E. Hurdle, Jr., *A Blow to Public Investing: Returning the System of Private Equity Fund Disclosures*, 53 UCLA L. REV. 239, 242–44 (explaining why privacy is so important in private equity firms).

[232] *See* Bamberger & Mulligan, *supra* note 14, at 298.

[233] *See* Westin, *supra* note 128, at 1F.

[234] *See id.*

over it" may make more sense.[235] Perhaps McNealy is a privacy unconcerned individual, and as such might not understand why people are so worked up about protecting their own privacy. If Westin is correct, then society should be particularly concerned about a sorting effect in which a disproportional number of corporate executives would fall in the privacy unconcerned portion of the spectrum. That would mean that the very people who do not understand what the privacy fuss is all about, are the decisionmakers making various crucial corporate decisions that impact employee and consumer privacy. In the worst case scenario, a corporate executive may entirely fail to recognize a privacy issue when the issue is not directly in front of them, but is buried in a decision that does not on its face appear to be about privacy. To use the language of law school professors, the privacy unconcerned corporate executive may not even spot the privacy issue on the exam.

Even, however, if corporate executives are just privacy pragmatists with lower valuations of privacy who have concluded that they are willing to take the tradeoff in their privacy in return for the many benefits of being a corporate executive, including money, prestige, and power, there are still reasons to be concerned. Even if the corporate executive is not all the way on the privacy unconcerned side of the spectrum, just having privacy be a low priority to them personally may impact corporate privacy decisions, as the result of a number of well-known behavioral and psychological phenomena increasingly recognized in the behavioral economics literature.[236] Alessandro Acquisti has extensively written about how various biases impact economic decisions in the privacy sphere.[237] He explains that "[d]ue to the uncertainties, ambiguities, and complexities that characterize privacy choices, individuals are likely influenced by a number of cognitive limitations and behavioral biases."[238]

For example, the social psychology literature suggests that there is a bias known as the false consensus effect by which individuals overestimate their similarity to others including unconsciously assuming that others share one's

---

[235] Sprenger, *supra* note 3.

[236] Behavioral economics generally studies how various individual, social, cognitive, and emotional biases influence economic decisions.

[237] *See, e.g.*, Alessandro Acquisti, *From the Economics to the Behavioral Economics of Privacy: A Note*, *in* ETHICS AND POLICY OF BIOMETRICS 23, 24 (Ajay Kumar & David Zhang eds., 2010); Alessandro Acquisti, *Nudging Privacy: The Behavioral Economics of Personal Information*, 7 IEEE SECURITY & PRIVACY 82, 83 (2009).

[238] Alessandro Acquisti & Jens Grossklags, *What Can Behavioral Economics Teach Us About Privacy?*, *in* DIGITAL PRIVACY: THEORY, TECHNOLOGIES, AND PRACTICES 363, 368 (Alessandro Acquisti et al. eds., 2007). Acquisti is largely talking about consumer privacy choices, but the logic he applies from the behavioral economics literature logically applies with equal force to the context of executives making privacy decisions within a corporation.

thoughts and values.[239] The research on the false consensus effect[240] originated in 1931, when a study found that admitted cheaters estimated the prevalence of cheating at a significantly higher rate than non-cheaters did.[241] Since then, the vast majority of hundreds of conducted studies have confirmed that individuals who engaged in a certain behavior, had a particular preference, struggled with a particular problem, or had a certain belief, assumed that others shared their characteristic when asked to estimate features about the general population, thus supporting the hypothesis that people overestimate the degree to which they are similar to others.[242]

Organizational behavior scholars have studied the impact of this false consensus effect on decision making within organizations. For example, one recent paper found that ethical decision making in organizations is subject to the false consensus bias by which individuals wrongly assume that others hold the same opinions regarding ethics as the individual.[243] Under this behavioral phenomenon, individuals' own views bias their estimates of the values held by the general population.[244] Perhaps resulting from a "desire for normative alignment," individuals within an organization become "predisposed to view their decisions as being more in line with the prevailing view than others' decisions are."[245] Additionally, the research found individuals view "alternative responses (particularly those directly opposed to their own) as deviant, or uncommon and inappropriate."[246] The authors explain that when ambiguity exists regarding the ethical action for the organization to pursue, individuals within an organization "will be inclined to see their actions as normative rather than deviant."[247] This effect may be exacerbated for individuals who play a central role in a social network because powerful individuals are less sensitive to the views of others.[248]

---

[239] *See* Jared Williams, *Financial Analysts and the False Consensus Effect*, 51 J. ACCT. RES. 855, 859 (2013) ("Ross, Greene, and House [1977] also investigated the phenomenon, and they were the first to use the term 'false consensus effect' to refer to it.").

[240] *See generally* Lee Ross et al., *The "False Consensus Effect": An Egocentric Bias in Social Perception and Attribution Processes*, 13 J. EXPERIMENTAL SOC. PSYCHOL. 279 (1977) (demonstrating the false consensus effect through a number of studies).

[241] DANIEL KATZ & FLOYD HENRY ALLPORT, STUDENTS' ATTITUDES: A REPORT OF THE SYRACUSE UNIVERSITY REACTION STUDY 205–35 (1931).

[242] Williams, *supra* note 239, at 859–60; *see also* Brian Mullen et al., *The False Consensus Effect: A Meta-Analysis of 115 Hypothesis Tests*, 21 J. EXPERIMENTAL SOC. PSYCHOL. 262, 261–63 (1985).

[243] Francis J. Flynn & Scott S. Wiltermuth, *Who's With Me? False Consensus, Brokerage, and Ethical Decision Making in Organizations*, 53 ACAD. MGMT. J. 1074, 1075 (2010).

[244] *Id.*

[245] *Id.*

[246] *Id.*

[247] *Id.*

[248] *Id.* at 1076.

Applying this research to corporate privacy decision making, it can be viewed as a subset of organizational ethical decision making more generally, and shares the characteristic that the correct privacy action for the organization to pursue is often ambiguous. Furthermore, corporate executives certainly play a central role within the social network of the corporation, and are the sources of power within the corporation. Consequently, this research suggests that the false consensus effect bias may cause corporate executives to wrongly assume that their various corporate constituents share the executives' low valuation of privacy. This causes them to incorrectly estimate the corporate constituent's views of the costs in a cost-benefit analysis of a particular corporate decision that may have privacy tradeoffs at stake.

Furthermore, the psychology and behavioral economics literature also suggests that individuals are likely to make decisions that validate their own prior life decisions as the result of a few related phenomenon. When facing a decision that suggests that an individual's prior life decision was incorrect, the individual subconsciously perceives cognitive dissonance.[249] As a solution to the cognitive dissonance, the individual makes use of confirmation bias and choice-supportive bias, in which the individual interprets objective evidence in a way that confirms our preferences, beliefs, and prior choices.[250] In this case, executives who have decided to trade away their own privacy, are more likely to conclude that others must be willing to trade away their privacy in return for some sort of benefit (such as the product or service the corporation is selling). Under this choice-supportive bias, individuals behave to retroactively justify their own life choices. Therefore, corporate executives who have already made the decision to trade-off their own personal privacy in pursuit of power, fame or fortune, then wrongly assume that everyone else is willing to similarly trade privacy in order to retroactively justify their life choices.

Both of these scenarios are exacerbated by the fact that, for the most part, neither employees nor consumers have meaningful choice when it comes to privacy. In other words, this supply-side explanation works hand-in-hand with the existing literature regarding the demand-side market failures explaining why corporations don't adequately protect privacy. The privacy sorting effect means that corporate executives are less likely to be concerned about privacy, and the demand-side market failures prevent them from being held accountable

---

[249] *See* Pauline H. Tesler, *Informed Choice and Emergent Systems at the Growth Edge of Collaborative Practice*, 49 FAM. CT. REV. 239, 243 (2011) (defining cognitive dissonance as "a state of tension that occurs whenever a person holds two cognitions (ideas, attitudes, beliefs, opinions) that are psychologically inconsistent . . . dissonance produces mental discomfort, ranging from minor pangs to deep anguish; people don't rest easy until they find a way to reduce it") (quoting CAROL TAVRIS & ELLIOT ARONSON, MISTAKES WERE MADE (BUT NOT BY ME) 13 (2007)).

[250] *See id.*

for that blindness. The supply-side corporate privacy market distortion and the demand-side consumer market failures are thus mutually reinforcing of the problem in that each failure permits the other to remain in the market.

It is also worth explaining how these various cognitive phenomena would occur within the inner working dynamics of various types of corporations. First, some "privacy merchant" corporations base their entire business model on buying and selling consumer data, and thus in a sense are in the privacy business.[251] These are not the corporations that are the focus of the theory of this Article. Privacy merchants are "bad" at privacy because it is their entire business model to be bad at privacy. There are no cognitive or other failures causing this result; they are accomplishing exactly what their business model intends.

Rather, this Article is focused on explaining corporations who are actually in the business of selling something else: cars, dolls, services, products, but along the way face numerous choices to prioritize or not prioritize privacy. Sometimes the choice is explicit, where everyone involved knows a privacy decision is being made. In scenarios with a conscious privacy decision the cognitive biases discussed above can play an important role. Corporations faced with such conscious privacy decisions may decide "wrong" regarding their expectation of consumer privacy preferences as a result of a combination of those biases. For example, a corporation facing a decision whether to take an action that they realize will have privacy consequences may have all the corporate executives ask themselves what decision they themselves would make if they were the consumer. Because they systematically are less likely to care about their own privacy, when they assume that their consumers likely match their privacy preferences they reach a decision that leads to a privacy failure. There is also likely a sort of group think phenomenon in which all the low-privacy valuing executives mutually reinforce the belief that consumers would also not care about making the privacy tradeoff at issue. Finally, this is further exacerbated by the choice-supportive bias, in which the corporate executives subconsciously desire to validate their life choices in which they have chosen to trade away their own privacy in exchange for the various benefits of their position. This may explain why there are so many anecdotal examples of corporations announcing privacy-invading decisions only to have to reverse course when they face a seemingly, but surprisingly unanticipated privacy backlash.

At other times, corporations may not even realize that the decision they are making is a privacy-implicating decision. This can occur at the top at the

[251] *See generally* Etzioni, *supra* note 29, at 930–32 (explaining the business model of "privacy merchants" and the vast extent to which these companies track Internet users).

level of the corporate leadership, or may occur further downstream as a result of a failure in the system design architecture. At the level of the C-suite, countless high-level corporate decisions may in some way implicate privacy, from a decision to install GPS trackers into company vehicles to a decision to store consumer data on a centralized database. Many such decisions however, do not obviously present themselves in the form of a privacy question. Put differently, the decisions are not framed in terms of should the corporation take this privacy-invading action, or should the corporation not take this privacy-invading action? Assume, for example that individuals, including corporate executives, who place a low value on privacy are not particularly concerned about GPS tracking, and in fact to use Westin's terminology, don't understand what the fuss is all about.[252] Therefore, in reaching a decision about installing GPS trackers, the conversation may focus on the financial costs, the efficiency costs, etc., but may not ever discuss the privacy costs to the employees because it doesn't reach their consciousness. A similar phenomenon can occur multiple times every day as corporations are faced with numerous seemingly innocent decisions that can have significant privacy consequences.

Other unintentional privacy decisions can take place further downstream within the corporate decision-making hierarchy, yet even these downstream decisions can be impacted by the privacy preferences of corporate executives. These downstream choices are what Harvard computer scientist Latanya Sweeney refers to as random design decisions.[253] A computer scientist or other engineer can design a product in a number of different ways in order to achieve many of the functional purposes of the product. To simplify, assume that one way of making a particular product is better for privacy, and a second way is worse for privacy. For example, a fitness wearable device could be designed in such a way that the individual's personal data is stored entirely on the user's own device (the Apple Watch), or it could be designed in such a way that the individual's personal data is stored on a centralized server (Fitbit). Similarly, a camcorder video camera can be designed with a mute button, or without a mute button. Corporations face countless such design decisions all the time.

---

[252] *See* Westin, *supra* note 128, at 1F.

[253] Latanya Sweeney, Dir., Data Privacy Lab, Harvard Univ., Keynote Session at the Amsterdam Privacy Conference: Must Intoxicating Technology be Toxic for Privacy? (Oct. 24, 2015); *see also* Latanya Sweeney, *Technology Science*, FED. TRADE COMM'N (May 2, 2014, 11:02 AM), https://www.ftc.gov/news-events/blogs/techftc/2014/05/technology-science [https://perma.cc/SL5L-A4LP] ("Multidisciplinary training . . . seems to be a way to increase . . . policy awareness among technologists, but may fall short of developing unified knowledge."); Latanya Sweeney, Visiting Professor, Harvard Univ. Ctr. for Res. on Computation & Soc'y, Hyperpublic, A Symposium on Designing Privacy and Public Space in the Connected World: The Hardest Challenges to Designing Privacy-Technology Solutions (June 10, 2011), *available at* https://www.youtube.com/watch?v=1vmjVMno2FI (view from the 11:03 timestamp for remarks on technology developers).

The low-privacy preferences of corporate executives can impact such downstream arbitrary design decisions in a number of different ways. First, at some corporations, often tech companies and former start-ups, there is a large cult of personality surrounding top corporate executives. Programmers and engineers are aware of the personality of the corporate executive, and in turn, without being explicitly told to do so, will make their various design decisions consistent with what they believe the executives would prefer. If, then, it is known within the corporation that the executives do not place a high priority or valuation on privacy, and don't really seem to understand why people care about privacy, then the engineers and computer scientists[254] will in turn make design decisions consistent with these presumed preference by the executives.

At other corporations, the issue may be one of software or process design architecture. Under such process design architecture, the corporate leadership is supposed to provide primary requirements and specifications for a product. For example, leadership can ask employees to design a watch that can be used to track employees' steps, and can also ask that it be made as quickly and cheaply as possible using the following specifications of size, weight, battery life, etc. If that design architecture fails to include any specifications regarding privacy, a likely result in the face of the low privacy preferences of corporate executives, then programmers or engineers are empowered to make arbitrary decisions that do not take into account privacy. This can be fixed by including privacy within the process design architecture, using what scholars have called "privacy by design,"[255] however, low-privacy valuing corporate executives are unlikely to recognize the need to do so. To really implement privacy by design, not only engineers making the design decisions need to be on board, but the corporate leadership must also prioritize "privacy by design" as part of the corporate culture.

III. Restoring Corporate Privacy

If there is a sorting phenomenon keeping individuals who place a high value on privacy out of corporate leadership, and if that sorting phenomenon is having a negative impact on corporate privacy decision making, then what can be done to counter that phenomenon?

Existing proposals for addressing systematic corporate privacy failures have focused on demand-side solutions both in terms of non-governmental

---

[254] There may even be reasons to think that the engineers and programmers themselves place a low value on privacy thus exacerbating the problem.

[255] *See* Rubinstein, *supra* note 18, at 1411 (explaining that "companies engage in privacy by design when they promote consumer privacy throughout their organizations and at every stage of the development of their products and services").

ways to address market failures, as well as legal interventions to protect the privacy of corporate constituents. These solutions will help to the extent that, as previously discussed, the demand-side issues exacerbate the problem by preventing corporations from being held accountable when they behave badly regarding privacy.[256]

In addition, however, if, as this Article theorizes, there is also a supply-side corporate privacy market distortion that is contributing to the problem, then supply-side reforms may offer an additional avenue for change. The rest of this Part offers two possible examples of such corporation-side reforms: one aimed at minimizing the sorting itself, and the second aimed at minimizing the impact of any sorting that occurs on corporate decision making.[257] First, to help combat the privacy sorting phenomenon itself, corporate disclosure laws could be modified to permit corporate executives to negotiate individualized personal disclosure policies, which would in turn be disclosed to shareholders. Second, in order to combat the impact of the privacy sorting on corporations, corporations could continue the trend of adopting CPOs as a necessary part of good corporate governance, in order to ensure that there is someone in the C-suite whose job it is to raise privacy concerns when making decisions.

A. Allow Executives to Negotiate Personal Disclosure Policies

As explained above, part of the structural problem that causes the privacy sorting phenomenon is that potential corporate executives are unsure whether various types of their personal information would need to be disclosed to shareholders. In light of this uncertainty, individuals who deeply value privacy may choose to pursue other business positions that would provide them more certainty in their ability to guard their own privacy. The simplest solution for this situation would be for the SEC to clarify that corporate executives do not need to disclose their personal information to shareholders. This is unlikely to occur, and potentially undesirable because counterbalancing the executives' privacy interest is a legitimate disclosure interest on the part of shareholders.[258]

---

[256] *See supra* notes 115–118 and accompanying text.

[257] A third supply-side possibility could involve reforming the curriculum at business schools to help teach good privacy practices, and help future corporate business leaders think about privacy as an integral part of all business decision making. *Cf.* Kevin T. Jackson, *The Scandal Beneath the Financial Crisis: Getting a View from a Moral-Cultural Mental Model*, 33 HARV. J.L. & PUB. POL'Y 735, 756–57 (2010) (suggesting the possibility of, and explaining the challenges with changing the business school curriculum to better teach business ethics in light of the prevailing business school "attitude that if something is not illegal then it must be acceptable"). I am certain there are numerous other possible supply-side reforms and welcome further efforts in this regard.

[258] *See* Schwartz, *supra* note 167, at 489 (arguing that "shareholders have a legitimate interest in disclosure of personal information about an executive that either impacts the ability of the executive to

Therefore, the best way to satisfy the shareholders' disclosure interest while allowing potential corporate executives to guard their privacy is to make a more minor change in the law to permit a two-step process: (1) mandatory contracting between the corporate executive and the corporation regarding the plan for the corporation's disclosures of the executive's personal information, combined with (2) mandatory disclosure of the negotiated disclosure plan to the shareholders.[259]

Under the first step, the law would be changed to not only permit, but also require corporate executives to negotiate their own personal disclosure policies when they are hired or promoted to their high-level position. Therefore the change would replace the strict traditional mandatory disclosure regime, which does not permit those executives with higher privacy preferences to negotiate to protect those preferences, with a mandatory contracting regime that allows executives with heterogeneous preferences to contract in a way consistent with those preferences. Under this contracting regime, high-level executives would contract with the corporation to determine the privacy disclosure policy that would apply to that executive's personal information in light of that executive's privacy preferences. This would allow potential executives who care about privacy to negotiate a disclosure policy that could adequately protect their privacy by treating privacy as one aspect of the overall compensation package that can be prioritized or traded off for other considerations.[260] The efficiency of the contracting regime could be facilitated by the creation of a menu of possible disclosure options, from which the parties could choose.[261]

Once the executive and corporation agree to a disclosure policy for that executive's personal information, the law would mandate the corporation to disclose the negotiated disclosure policy to the shareholders, in order to protect and balance the shareholder interest in disclosure of relevant information. In other words, the corporation would disclose to shareholders whether or not it would in the future be disclosing personal information about a particular high-level executive to the shareholders, thus allowing shareholders to decide whether, and how much they value that information.

For example, assume a high-level executive and a corporation bargain for a privacy policy from among the menu of choices that is fairly protective of privacy. The policy may say, perhaps, that the corporation will not disclose personal information about the executive unless it is currently substantially

---

currently perform his or her duties, or is likely to impact the executive's ability to perform his or her duties in the future").

[259] *See id.* at 517.

[260] *Id.* at 517–24.

[261] *See id.* at 520 (describing how the menu approach could work).

impacting his or her ability to do his or her job, and even then the corporation will only disclose the fact of the impairment, not the underlying personal facts. The corporation would then be required to disclose this disclosure policy to the shareholders. If shareholders do not find this level of disclosure adequate, then the market can respond accordingly, and protection of privacy can be factored in to market forces, just like increased salaries, or any compensation feature desired by executives. The menu approach would help facilitate the usability of this system, as implementing a standard format and common vocabulary across disclosure policies would allow shareholders to directly compare disclosure policies. It could also be designed to be relatively straightforward, rather than taking the form of the lengthy legalese privacy policies that consumers are given and ignore all the time. This would help solve the sorting problem by increasing the likelihood that individuals who value privacy would consider pursuing corporate executive positions.

B. Make Chief Privacy Officers Part of Good Corporate Governance

The solution above may reduce the corporate privacy sorting problem, but it cannot remove it entirely. This is because the disclosure requirements are only one of the ways in which the privacy of executives is compromised in addition to the role of the public and media in wanting and providing personal information about corporate executives.[262] Thus any solution that aims to restore functional supply-side corporate decision making with regard to privacy must also target the impact of the remaining sorting problem. One way to counter the sorting phenomenon is for corporations to be encouraged to take steps to make sure that the privacy-valuing perspective is actually represented in the corporate boardroom.

This lends additional support to those who have already spoken about the positive benefits of CPOs within the corporate structure. One of the best ways to make sure the privacy perspective is heard is to make the existence of a CPO a defined part of good corporate governance practices. As Peter Swire opined based on his prior experience as essentially the CPO for the Federal government:

> I believe having a person visibly responsible for privacy is a helpful way to ensure that privacy issues are considered in the organization's actions. Privacy concerns may or may not win out in the eventual decisions, but having a person expert in privacy in the process means

[262] It is far less likely that the courts would shift First Amendment or defamation doctrine in such a way that would permit corporate executives to protect their personal privacy from the public and the media.

> that the other participants at least have to articulate why the proposed actions are consistent with the organization's announced privacy policies.[263]

Swire's insight becomes even more important if there are reasons to believe that the rest of the C-suite is disproportionately unlikely to adequately consider or value privacy issues.

CPOs already exist at many corporations for a variety of reasons. In the early 1990s a number of industries such as telecom, health, and information technology began facing great risks with data collection and processing.[264] These industries began assigning employees the task of managing privacy.[265] By the mid-1990s, Jennifer Glasgow at Acxiom made the shift from the leader of the company's privacy efforts, to officially holding the title of CPO.[266] Other companies created similar positions during the 1990s.[267] Often, the creation of high-level corporate privacy positions was triggered by a crisis, which required the corporation to convince skittish consumers that corporations were not "a lot of evil-headed monsters."[268] For example, in response to some trouble DoubleClick announced in 2000 that they were going to create a CPO role.[269] At the time, Crain's New York Business mocked the CPO title and predicted its demise.[270] Instead, in November 2000, Harriet Pearson became the first CPO of a Fortune 100 Company,[271] and by 2001, the New York Times reported that CPOs had become increasingly common in the C-suite with over one hundred such positions in the United States.[272]

---

[263] Peter P. Swire, *The Surprising Virtues of the New Financial Privacy Law*, 86 MINN. L. REV. 1263, 1316–17 (2002). Swire served as Chief Counselor for Privacy in the U.S. Office of Management and Budget. *Id.*

[264] Andrew Clearwater & J. Trevor Hughes, *In the Beginning . . . An Early History of the Privacy Profession*, 74 OHIO ST. L.J. 897, 904 (2013).

[265] *Id.*

[266] *Id.*

[267] *See* Swire, *supra* note 263, at 1316 n.199 (noting that Ray Everett-Church began using the CPO title in September 1999).

[268] Bamberger & Mulligan, *supra* note 14, at 262 (conveying a quote by Microsoft CPO Richard Purcell as quoted in John Schwartz, *Conference Seeks to Balance Web Security and Privacy*, N.Y. TIMES (Dec. 8, 2000), http://www.nytimes.com/2000/12/08/business/conference-seeks-to-balance-web-security-and-privacy.html?_r=0 [https://perma.cc/UH68-J7RA]).

[269] Clearwater & Hughes, *supra* note 264, at 905.

[270] *Id.*

[271] *Id.* at 906.

[272] John Schwartz, *First Line of Defense; Chief Privacy Officers Forge Evolving Corporate Roles*, N.Y. TIMES (Feb. 12, 2001), http://www.nytimes.com/2001/02/12/business/first-line-of-defense-chief-privacy-officers-forge-evolving-corporate-roles.html [https://perma.cc/6M7P-VA4R]; *see also* Michelle Kessler, *Position of 'Privacy Officer' Coming into Public Eye*, U.S.A. TODAY, Nov. 30, 2000, at 1B (pointing out that the number of companies with CPOs had gone from zero to seventy-five).

In addition to various privacy crises triggering the creation of a CPO role, the other leading factor in the rise of the prevalence of the CPO originated in Europe.[273] In 1995, the EU Data Privacy Directive attempted to implement common multinational data security law across the European Union.[274] U.S. companies began to address this law, which limited data from leaving Europe unless the importing country had "adequate" protections in place.[275] Because Europe considered the American data privacy protections inadequate under European standards, American companies needed to figure out a way to obtain important data for their companies.[276] The resulting complexity drove the rise of CPOs.[277]

Other factors may also have played contributing roles in the rise of the CPO. According to Swire, the Gramm-Leach-Bliley Act of 1999 ("GLB"), a financial privacy law, also played an underappreciated role in the rise of the CPO.[278] Swire argues that the privacy notice requirements of the GLB coupled with liability for violating those privacy notices required a larger compliance effort than has been recognized, and that resulted in the number of CPOs rising rapidly in the aftermath of the GLB.[279] Additionally, Andrea Matwyshyn points out that for industries involving health data privacy, under HIPAA, covered entities must designate a privacy official to be responsible for developing and implementing the entity's policies and procedures.[280] Others have suggested that the rise of the FTC privacy enforcement and the corresponding threat of FTC oversight inspired some corporations to hire a privacy officer,[281] and led to increased corporate reliance on professional privacy management.[282]

Regardless of the varied motivations for the rise of the CPO thus far, the theory developed in this Article supports the benefits of the continued rise and entrenchment of the CPO in corporate governance. Bamberger and Mulligan have studied how corporations actually manage privacy and what motivates

---

[273] Clearwater & Hughes, *supra* note 264, at 909.

[274] *Id.*

[275] *Id.*

[276] *Id.* at 909–10.

[277] Bamberger & Mulligan, *supra* note 14, at 262.

[278] *See* Swire, *supra* note 263, at 1316.

[279] *See id.* at 1317.

[280] Andrea M. Matwyshyn, *Material Vulnerabilities: Data Privacy, Corporate Information Security, and Securities Regulation*, 3 BERKELEY BUS. L.J. 129, 155–57 (explaining that HIPAA regulations are part of Congress's attempt to "legislate information security").

[281] Bamberger & Mulligan, *supra* note 14, at 274 (basing their findings on "qualitative interviews with chief privacy officers identified by their peers as industry leaders").

[282] *Id.* at 294 (explaining that "the combination of uncertainty regarding the FTC's evolution of privacy requirements and uncertainty regarding market responses spurred by data breach notifications was central to the striking trend towards corporate reliance on professional privacy management").

them.[283] Specifically, they studied the corporate attitudes and practices of those corporations who had been identified as industry leaders with regard to privacy based on interviews with the CPOs of those leading companies.[284] Despite the admitted limitations of their methodology, at the very least their results are consistent with the idea that having a CPO within the corporate boardroom can compensate for the lack of privacy issue spotting that might otherwise occur. Consistent with what this Article would predict, their study found that those corporations identified within the industry as having the best privacy practices involved a CPO who was able to get onto the corporate board's agenda, who had high status within the corporation as a privacy leader, and who was able to managerialize and institutionalize privacy as part of privacy by design.[285] The CPOs within the Bamberger and Mulligan study,[286] expressed a consistent theme that suggested their role in pushing privacy policies to the forefront of strategy within the corporation and being proactive and predictive. One such CPO pointed out that the ambiguity inherent in privacy regulation as a highly evolving area, means the CPOs' role consists of "[l]ooking around corners . . . looking forward to things that are a few years out."[287] Another CPO explained, "Customer expectations change and the employee expectations change. The world changes periodically too on top of that and I look at what we're doing as something that's really important from any kind of a personal and values perspective and from a business perspective."[288] A third CPO explained that the focus is on "the next thing that's coming down the pike, because if you get caught unawares, you're behind the ball and you're spending a lot of money."[289] In the absence of clear rules and industry standards, which would be very difficult given how quickly privacy norms can change, for a corporation to be proactive and predictive on issues of privacy requires an individual in the corporate boardroom responsible for thinking about and raising these privacy issues. This theory offered by this Article suggests that the traditional C-suite would not be able to foresee these issues themselves.

The benefits of having CPOs as a matter of good corporate governance to offset the privacy indifference of corporate executives more generally increase with the rise of a professionalized privacy-officer community. To the extent

---

[283] *Id.* at 249.

[284] *Id.* at 252, 263.

[285] BAMBERGER & MULLIGAN, *supra* note 56, at 15.

[286] There may be a bias on the part of the interviewed CPOs to overemphasize their role in the corporations' privacy successes in order to advance their own status. The Bamberger and Mulligan study is not used to prove the point regarding the helpfulness of CPOs, but rather merely to point out that the two are consistent.

[287] Bamberger & Mulligan, *supra* note 14, at 271.

[288] *Id.*

[289] *Id.* at 272.

that CPOs face struggles in the C-suite with other corporate executives who either don't recognize the privacy issue, or don't understand its importance, they are able to network with other professionals within the privacy-officer community to increase traction. CPOs in Bamberger and Mulligan's studies reported that information obtained from peers provided leverage as they advocate for certain privacy practices within their own firms.[290] At times they even reported being brought in to communicate with other corporations to help convince a reluctant executive committee about the benefits of a particular privacy initiative.[291] One CPO recalled the following:

> I've been on the phone with [other firms'] executive committees, telling them about [our company's] experience because it helps the other company['s] privacy office to have me tell their people because they've told them and they don't believe them. So when they hear it directly from me, that has some advantage and I've done that with a number of different companies.[292]

Interestingly, the CPOs did not view privacy as a competitive feature upon which corporations can distinguish themselves to obtain an advantage in the market.[293] Rather, they viewed privacy as having a network effect by which a competitor's privacy mistake risked tarnishing the industry and a competitor's privacy successes add value to an entire industry that exceed the competitive advantage to any particular firm.[294] Consequently privacy professionals were willing to freely share information about privacy policies and practices.[295]

Reasonable minds can disagree precisely how to increase and continue to promote the rise of CPOs. One possibility is merely to promote the CPO as a matter of good corporate governance. Alternatively, it is possible to use more coercive and governmentally mandated mechanisms. Regardless of which mechanism is used, the corporate-market distortion theory offers good reason to believe that consistent with the evidence obtained thus far, the increased use of CPOs who are well integrated into a corporation and with the actual power to raise privacy concerns will help offset some of the corporate privacy failures that occur as the result of the privacy sorting phenomenon.

---

[290] *Id.* at 278.
[291] *Id.*
[292] *Id.*
[293] *Id.*
[294] *Id.*
[295] *Id.* It might be worth considering whether there may be some anti-trust concerns with this behavior. That argument is beyond the scope of this paper.

CONCLUSION

This Article presents an additional theory for corporate privacy failures that focuses on market distortions within the corporation itself starting at the very top with the CEO and other members of the C-suite. This theory is meant to complement rather than replace the theories offered by the existing literature that exclusively focus on demand-side market failures. Admittedly, the theory offered in this Article is purely theoretical. The Article has described a possible theory and presented reasons drawn from the privacy, behavioral psychology, and economic literatures that suggest reasons that such a theory may help offer a more complete explanation for corporate privacy behavior. In future work, it is possible to collaborate with empirical scholars to better test aspects of this theory.

One imperfect, but plausible option to test the privacy sorting aspect of the theory would be to conduct surveys of top business school students asking them both about their career goals and previously established questions to help determine their privacy preferences. If the privacy sorting theory is correct, then such a study should be consistent with a hypothesis that business school students who care about privacy are less likely to aspire for positions in the C-suite of publicly traded companies, and instead plan to pursue other fields such as banking, management consulting, and hedge funds. Although not a perfect measure, this might be a more feasible project in lieu of the unlikely strategy of trying to get corporate executives to respond to surveys in a reliable fashion.

Another possibility would be to look at publicly available indicators of the privacy preferences of corporate executives. This could include the publicly available social media presence of corporate executives prior to the time that they became corporate executives. By looking closely at whether the corporate executive had a social media account such as Facebook, whether that account is limited to friends or is viewable by the public, and the degree to which the executive shares personal information on their social media account, it may be possible to get a rough sense of the privacy preferences of corporate executives. Partners at management consulting firms, banking companies, and hedge funds might be used as a baseline of comparison to determine how corporate executives compare with other high-level jobs with regard to social media. Other indicators might include considerations such as whether the executives wrote an autobiography, the number of images that come up in a Google search that are personal in nature, whether the executive has invited the public into their personal lives in any way, such as with a popular media interview, etc.

Of course, there are likely other ways to test aspects of the theory, and any efforts by others to do so are encouraged as proof of the validity of the hypothesis will help inform various policies and legal debates regarding how

to treat privacy in our society. Most importantly, if the corporate-side privacy market distortion theory is correct, then consumer-side solutions will not alone suffice to fix the corporate privacy problem. Solutions must also tackle the lack of privacy in the C-suite.