6-18-2019

Response to McGeveran's The Duty of Data Security: Not the Objective Duty He Wants, Maybe the Subjective Duty We Need

Gus Hurwitz
University of Pennsylvania Carey Law School, ghurwitz@law.upenn.edu

Response

Response to McGeveran's *The Duty of Data Security*: Not the Objective Duty He Wants, Maybe the Subjective Duty We Need

Justin (Gus) Hurwitz†

INTRODUCTION

William McGeveran's recent article, *The Duty of Data Security*, is a significant contribution to ongoing debates about what duty firms holding electronic information about consumers owe in ensuring the security of that data.[1] It also supports the opposite conclusion from that which McGeveran articulates. McGeveran frames the article as identifying a clear duty of data security. This response argues that in his efforts to locate a clear duty in existing data security law he has identified a standard that, in all meaningful ways, is one of subjective (not objective) reasonableness – and therefore offers no clarity at all. There is likely room for disagreement on both sides of this argument – both that which McGeveran makes and my response to it. The ultimate purpose this this response, however, is to recognize this aspect of the duty that McGeveran has identified and to reframe it in the familiar terms of objective vs. subjective reasonableness. This distinction is both useful and important, and has gone unremarked upon in two decades of discussions about the data security obligations.

† Associate Professor of Law and Co-Director, Space, Cyber, and Telecom Law Program, University of Nebraska College of Law and Director of Law & Economics Programs, International Center for Law & Economics; Program Affiliate NYU School of Law Classical Liberalism Institute. JD, University of Chicago, 2007; MA, George Mason University (economics), 2010; BA, St. John's College, 2003. The author has written several articles and amicus briefs critical of the FTC's approach to data security. With thanks to Justin McCully for helpful research assistance and Bill McGeveran for being receptive to and supportive of this response.

1. William McGeveran, *The Duty of Data Security*, 103 MINN. L. REV. 1135 (2019).

McGeveran is responding to arguments that any duty of data security created by the law is "insufficiently specific, concrete, or uniform," and that "there is no way to understand the meaning of 'reasonable' data security measures under consumer protection law."[2] Presumably in the interest of jocular and spirited debate, he calls such claims "balderdash." The purpose of his article is to support his claim of "balderdash" – to argue that many "duties" of data security are found throughout the law and that these "numerous sources of a duty of data security sound together in harmony, not cacophony."[3]

To this end he undertakes the yeoman's task of surveying a large cross-section of American law as it pertains to data security. He looks, in total, at 14 different areas of law – including seven areas of public law and seven areas of private law – and distills from this survey a range of commonalities that exist across this body of law.[4] He then synthesizes from these commonalities the attributes of what he calls a duty of data security.[5] This "duty," however is largely meaningless because it is one of *subjective* reasonableness. Though it has not been framed in these terms, a significant part of the data security debate over the past decade has been about whether data security is governed by an *objective* reasonableness standard.[6] By situating the duty of data security in subjective reasonableness, McGeveran effectively torpedoes the arguments of the enforcement advocates to whom he believes he is an ally.

The rest of this response proceeds in three parts. Part I briefly summarizes McGeveran's article, emphasizing the vast areas of agreement between us. Part II then turns to disagreement, explaining that the core of the duty that he identifies is largely meaningless – imposing no enforceable burden on any but the largest or the most egregious of data security offenders. Part III then takes a step back to ask the most important question of data security that lawyers never ask: why does the duty of data security matter? This question helps us to calibrate what the duty of data security *should* be. The answer, it turns out, tells us that the standards that McGeveran has identified as prevalent today are well calibrated to the problems they should be trying to solve – much to the chagrin of enforcement agencies

2. *Id.* at 1136.
3. *Id.* at 1137.
4. *Id.* at 1139.
5. *Id.*
6. See *infra* Part II.A.

who would prefer objective data security standards. In the end, this leaves us in perhaps a curious place of agreement: the duty of data security that McGeveran articulates is not the one that he wants, but it may be the duty that we need.

I. MCGEVERAN'S ARGUMENT, AND WHERE WE AGREE

McGeveran's article offers a masterful descriptive analysis of vast swaths of current data security law. Roughly the first half of his article is a survey of the dominant public and private law frameworks for regulating data security.[7] This includes, for instance, HIPAA and GLBA, FTC enforcement through its consumer protection authority, state laws and regulations, industry self-regulation, professional certification, and contractual mechanisms. Other than its exclusion of common law mechanisms – a reasonable exclusion given the uncertain and to date largely ineffective status of common law tools in regulating data security practices – this is without a doubt the most comprehensive current survey of data security law.

Part II of McGeveran's article offers his core analysis, synthesizing common characteristics across the regimes surveyed in the first half of the article to identify the core "content" common across all of these regimes.[8] He breaks this analysis down into four parts, the first two of which reflect canonical understandings and the latter two of which are at least very interesting. The central element of the "duty of data security" that he identifies relates to reasonableness and risk.[9] As he describes it, "all the frameworks [considered in Part I] embrace some form of a reasonableness requirement, whether or not using that name."[10] I will return to his discussion of reasonableness as the defining element of the duty of data security in Part II below – for now, it suffices to say that I agree with his identification of reasonableness as central, but believe that it mischaracterizes the nature of reasonableness embodied in this standard.

The second conceptual element that he identifies is that data security is built around what he calls "systems of compliance."[11] This, too, is common understanding within the field – more commonly phrased as security is about process, not state. In other words, good security requires continual identification,

7. McGeveran, *supra* note 1, at 1141–75.
8. *Id.* at 1175.
9. *Id.* at 1176.
10. *Id.* at 1175.
11. *Id.* at 1180.

assessment, monitoring, responding, and improvement – it is not about achieving a state of being secure, but is about approaching security as on ongoing activity.[12] This is best captured from a regulatory perspective, for instance, by the HHS OCR's general emphasis in HIPAA compliance on whether a firm that may have experienced a security incident had security procedures in place and *not* whether those procedures were substantively good.

The third conceptual element that McGeveran identifies is interesting, if less compelling. He identifies three architectural components of good data security practices: access controls, encryption, and multi-factor authentication.[13] Substantively he overstates his case. For instance, implementing access controls is better characterized as part of the process that makes up a system of compliance. That this is a process- or system-level element is indicated by the fact that the extent of access control requirements needs to be scoped to the systems or data to be protected (that is, any system that implements absolute access controls would be unusable). Similarly, with multi-factor authentication, which is an aspect of an access control implementation – some system components need no authentication, others may reasonably only need a single factor of authentication, while others may need multiple factors (and even continuous affirmation) of authentication. Encryption is an even more contentious element for McGeveran to identify as a clear architectural element of data security. Not all the frameworks he considers, for instance, require all data to be encrypted in all circumstances, and from a compliance perspective encryption safe harbors (common in many of the frameworks) have been criticized as leading to overall poorer security environments.[14]

The fourth conceptual element McGeveran identifies – "worst practices" – is notably interesting and reflects ongoing discussion within the community about applying concepts such as *per se* negligence to address overtly problematic conduct that

12. *Id.* at 1183.

13. McGeveran, *supra* note 1, at 1189–93.

14. *See, e.g.*, U.S. Department of Health & Human Services, *Health Information Privacy*, HHS.gov (Jul. 26, 2013), https://www.hhs.gov/hipaa/for-professionals/faq/2001/is-the-use-of-encryption-mandatory-in-the-security-rule/index.html ("Is the use of encryption mandatory in the [HIPAA] Security Rule? Answer: No."; PCI-DSS Requirement 4 ("Sensitive information must be encrypted during transmission *over networks that are easily accessed by malicious individuals*.") (emphasis added). *See also* David Thaw, *The Efficacy of Cybersecurity Regulation*, 30 GA. ST. U. L. REV. 287 (2013) (discussing how encryption safe harbors can lead firms to invest uncritically in encryption technology, at the expense of investment in other security resources).

falls below any arguable understanding of reasonable security.[15] This is a developing area of discussion and McGeveran's characterization of these practices is in line with much current thinking.

Importantly, the idea of *per se* negligence for such clearly problematic "worst practices" is complementary to the standard of reasonableness discussed in the rest of this response. As discussed below, the standard of reasonableness that McGeveran identifies (and discusses as the first conceptual element of data security) is a *subjective* standard, not an *objective* one. This is reflected in the characteristics that define the concept of reasonableness throughout the various frameworks that he surveys and by the centrality of process (or "systems of compliance" in McGeveran's terminology) in understanding the duty of data security.[16] The evolving, and increasingly accepted, norm for good data security is for firms to adhere to an exceptionally low baseline of minimal practices and, beyond that baseline, to engage in reasonable effort to secure their systems (that is, to try to be secure, regardless whether they succeed).[17] This roughly corresponds to a subjective reasonableness standard backed by a *per se* negligence standard for extremely objectionable conduct.

But I get ahead of myself – I will return to these ideas after further discussion of the McGeveran's duty of data security.

Part III of McGeveran's article offers his normative assessment of the duty that he identifies. The rest of this response is in dialogue with that assessment.

II. MCGEVERAN'S DUTY OF REASONABLENESS IS MEANINGLESS

Given the extent to which I agree with McGeveran, it may be surprising that I find his article fundamentally flawed. But, alas, I do! The reason is that in his effort to identify whether a duty of data security exists and to articulate it, he fails to consider the purpose of that duty – and whether the standard he identifies satisfies that purpose. In other words, he misses forest for the trees.

15. McGeveran, *supra* note 1, at 1193–95.

16. *Id.*

17. *See, e.g.*, Derek Bambauer, Cybersecurity for Idiots (Mar. 16, 2016) (unpublished article) (on file with the author) (arguing that "cybersecurity should develop a jurisprudence of negligence *per se* rather than of negligence.").

A. WHAT IS THE DUTY OF DATA SECURITY DEBATE?

The animating issue in the debate about the duty of data security is not whether such a duty exists. It is whether that duty is based on an objective or subjective standard that can be applied economy-wide. The focal point of this debate has been the Federal Trade Commission's efforts to develop a "common law" of data security based upon its broad Section 5 "unfairness" authority.[18] This effort was crystalized in the Commission's efforts to act against LabMD, a small medical testing laboratory that allegedly experienced a data breach in 2008.[19] As McGeveran's article was nearing completion, the 11th Circuit court of appeals issued its opinion in LabMD's final appeal of the FTC's efforts in that case, vindicating LabMD's arguments that the FTC's data security standard was unenforceable vague and vacating the FTC's decade-long case against LabMD.[20]

In its efforts to develop these standards, including in litigation against LabMD, the FTC has analogized the standard it applies in data security cases to that of negligence in the tort setting (that is, of objective reasonableness).[21] Critics of the FTC's objectiveness standard, myself included, have argued, in effect, that there is no *objective* standard or reasonableness in the data security context and that any subjective standard is fundamentally unavailing in a generalized, economy-wide, context. In its opinion the 11th Circuit agreed. The 11th Circuit characterized the central provision of the Commission's order against LabMD as subject to "an indeterminable standard of reasonableness," and characterized five other commands in that order as "equally vague."[22]

In other words, because the FTC's order provides no objective standard by which the court can evaluate the reasonableness of LabMD's data security efforts, the court would be forced to evaluate compliance with that order on an ongoing, case-by-case, basis.[23] In particular, the court explains, the FTC's order "is devoid of any meaningful standard informing the court of what constitutes a 'reasonably designed' data-security program."[24] That is, because there is no objective standard by which

18. *See* LabMD, Inc. v. FTC., 894 F.3d. 1221, 1231–32 (11th Cir. 2011).
19. *Id.* at 1224–27.
20. *Id.* at 1237.
21. *Id.* at 1231.
22. *Id.* at 1236, n.41.
23. *Id.* at 1236–37.
24. *Id.* at 1236.

the court can evaluate compliance with the order the court cannot enforce the order.

The 11th Circuit was concerned with the judicial enforceability of the FTC's orders. But the same concern trickles down to the firms regulated by the FTC—literally every business in the country. Most businesses are no more expert in data security than a typical judge. Indeed, courts are assisted by expert witnesses and extensive briefing on the specific issues before them. If the standard proffered by the FTC is too indeterminate for a court to objectively evaluate conduct in specific cases, then clearly it is too indeterminate to be applied in the general case. Indeed, this is part of the reason that other judges had raised concerns about the FTC's data security efforts on due process grounds.[25] That is, it is an inherently subjective, not objective, standard.

B. MCGEVERAN'S COMPELLING CASE FOR A SUBJECTIVE STANDARD

The LabMD case, of course, is just one data point. The structure of the 11th Circuit's opinion is fairly characterized as "curious." The 11th Circuit's focus on the judicial enforceability of the Commission's order is an awkward sidestep of a direct evaluation of the Commission's substantive authority.[26]

Fortunately, McGeveran has undertaken the arduous task of comprehensively surveying data security law as it exists across the country.[27] What he overwhelmingly finds is that it is subject to a *subjective* reasonableness standard. Consistent with the 11th Circuit, such a standard is exceptionally difficult to enforce through the legal system.

Throughout his survey of data security standards, McGeveran comes across myriad examples of reasonableness standards. Importantly, McGeveran does not explicitly distinguish between objective and subjective reasonableness.[28] He does offer a brief discussion of the concept of reasonableness, noting that "Perhaps the most prominent reasonableness standard

25. *See Generally* J. William Binkley, *Fair Notice of Unfair Practices: Due Process in FTC Data Security Enforcement after Wyndham*, 31 BERKELEY TECH. L. J. 1079 (2016) (discussing the due process concerns, especially fair notice, related to FTC enforcement actions).

26. I would hazard to guess that the court took this approach to avoid addressing difficult questions about the constitutionality of the Commission's substantive legal authority.

27. *See generally* McGeveran, *supra* note 1, at 1141–58.

28. McGeveran, *supra* note 1, at 1176–79.

in law is the general measure of liability for negligence torts," and citing to the Restatement of Torts' definition of reasonableness.[29] Tellingly, while he cites the Restatement comment that discussed the "Qualities of the 'reasonable man,'" he omits the subsequent comment on the "Standard of the 'reasonable man."[30] This subsequent comment explains that:

> Negligence is a departure from a standard of conduct demanded by the community for the protection of others against unreasonable risk. The standard which the community demands must be an objective and external one, rather than that of the individual judgment, good or bad, of the particular individual.[31]

In other words, tort law's negligence objective reasonableness standard is atypical; more often reasonableness is adjudged on a subjective basis.

Curiously, McGeveran takes a moment to chastise the 11th Circuit for importing the tort negligence standard—one based on objective reasonableness—into the LabMD case.[32] McGeveran responds to this concern by distinguishing the tort negligence standard from the reasonableness standard he finds across data security law.[33] As an example of the "reasonableness" standards, he cites examples where reasonable data security is defined, for instance, in terms of requiring "each company to assess its specific risk profile and design a program that addresses its risks in a robust fashion."[34] He then goes on to cite the NIST Cybersecurity Framework as another example:

> With this information, organizations can determine the acceptable level of risk for achieving their organizational objectives and can express this as their risk tolerance. With an understanding of risk tolerance, organizations can prioritize cybersecurity activities, enabling organizations to make informed decisions about cybersecurity expenditures.[35]

McGeveran doesn't cite the FTC's typical language in describing its data security expectations, but they are similar, modeled after the data security requirements in HIPAA and GLBA (which he does cite).[36] The specific language, for instance,

29. McGeveran, *supra* note 1, at 1196, n.324.

30. RESTATEMENT (SECOND) OF TORTS § 283, cmt. b (AM. L. INST. 1965).

31. *Id.* at § 283, cmt c.

32. *Id.* at 1176.

33. *Id.* at 1178–79.

34. *Id.* at 1178 (citing N.Y. COMP. CODES R. & REGS. tit. 23, § 500.00 (2018)).

35. *Id.* (citing NAT'L INST. OF STANDARDS & TECH., FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY 4 (2018), https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018 .pdf.

36. *See id.* at 1148, 1170.

from the FTC's LabMD order noted by the 11th Circuit is:

> [T]he respondent shall . . . establish and implement, and thereafter maintain, a comprehensive information security program that is reasonably designed to protect the security, confidentiality, and integrity of personal information collected from or about consumers . . . . Such program . . . shall contain administrative, technical, and physical safeguards appropriate to respondent's size and complexity, the nature and scope of respondent's activities, and the sensitivity of the personal information collected from or about consumers . . . .[37]

"Company specific risk profiles"? "Achieving organization objectives," "risk tolerance," and "prioritizing cybersecurity activities"? "Safeguards appropriate to [] size and complexity"? These are requirements that firms tailor their security programs to their specific circumstances, based on firm-specific assessments. This is the language of *subjective* reasonableness.

Ultimately, it seems likely that McGeveran would agree that the reasonableness standard he finds situated in his survey of data security standards has elements of subjective reasonableness. Indeed his articulation of the duty of data security emphasizes that that duty is rooted in flexible standards and calibrated to the risks faced by and resources available to the firm holding data.[38]

III. THE QUESTION NOT ASKED: WHY DOES THE DUTY OF DATA SECURITY MATTER?

The greatest failing of the academic and regulatory discussion about data security is its failure to consider why liability for data security failings matters. This question is predicate to questions about what the duty to secure data should be. Rather, the trajectory of discussion about the duty to secure data has progressed in a less thoughtful, more legalistic manner: Data breaches occur resulting in harm to the owners of whatever data was compromised; liability is the legal remedy to that harm. Under our standard theories of remedies, imposing liability both makes the harmed parties whole *ex post* and creates incentives *ex ante* for data custodians to invest in precautions to protect data from future compromise.

But this is not how things play out in the data security context. What constitutes "reasonable" data security is so indeterminate that the vast majority of firms have little ability to invest

37. For completeness, HIPAA's Security Rule requires firms to implement security measures in proportion to "The size, complexity, and capabilities of the covered entity or business associate." 45 C.F.R. § 164.306(b)(2)(i).

38. McGeveran, *supra* note 1, at 1179.

in precautions prudently. To be sure, there are "worst practices" that may reasonably be the basis for liability; and large firms may be sufficiently sophisticated and well-resourced to be considered sophisticated security actors.[39] But for the majority of firms, liability for a data security incident is purely random. And, it turns out, that in terms of incentives this is the worst of all possible worlds: for these firms either a strict liability or a no liability rule would be far superior to a "reasonableness" standard – for both the firms and general data security practices.

A. HACKERS GONNA HACK. BUT WHY?

The starting point for understanding what a duty for data security should be is understanding what that duty is responding to. Security compromises occur in an adversarial setting; a compromise means that a third party has been able to access information stored on a data custodian's systems without authorization. The duty of data security, therefore, is not about ensuring that that custodian keeps data in a locked box. Every locked box has vulnerabilities and in the adversarial cybersecurity setting threat actors and others are constantly searching for new vulnerabilities and new ways to exploit known vulnerabilities. The duty of data security, therefore, is more akin to keeping apace of advancements in the field of cybersecurity, of constantly monitoring, updating, testing, and replacing the locked box that data is secured into.

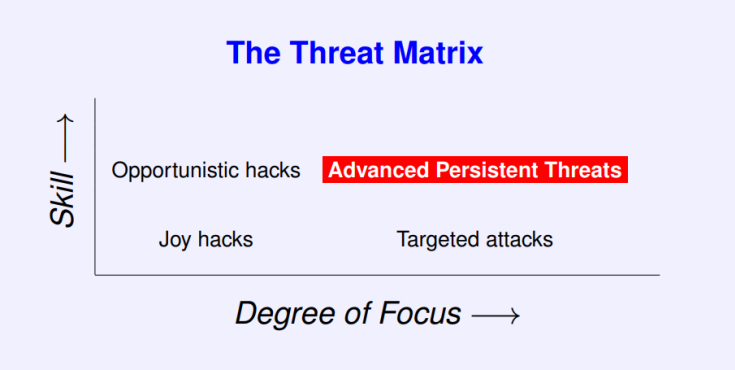
We can better understand what this duty should entail by looking at who these threat actors are—including what their motivations are. Steven Bellovin categorizes threat actors along two dimensions, as seen in Figure 1.[40] One dimension measures the skill of the attacker; the other measures the extent to which the attacker focuses on a specific target. From this, he identifies four categories of attackers.[41]

39. *See* Justin (Gus) Hurwitz, *The FTC's Data Security Error: Treating Small Businesses Like The Fortune 1000*, FORBES (Feb. 20, 2017, 8:00 AM), https://www.forbes.com/sites/washingtonbytes/2017/02/20/the-ftcs-data-security-error-treating-small-businesses-like-the-fortune-1000/#7769fb4b5a82.

40. *See* STEVEN M. BELLOVIN, THINKING SECURITY: STOPPING NEXT YEAR'S HACKERS 34 (Brian W. Kernighan ed., 2015).

41. *See id.* at 31.

Figure 1: Steven Bellovin's Threat Matrix



First are "Joy Hackers," who are neither sophisticated nor focused, but rather attack firms on an ad hoc basis where the opportunity arises, using the tools in their existing skill set.[42] Their motivation is, as the name suggests, the sheer joy of hacking. These individuals generally represent the threat model of the 1990s, when there were far fewer systems connected to the Internet and less thought was given to securing them at all. They do not need to seek out targets or develop innovative ways into the systems of whatever targets they find.[43] Rather, they have enough sophistication to recognize obvious vulnerabilities as they happen upon them and exploit them on an ad hoc basis for little reason other than because they can.[44]

Moving to the right on Figure 1, "Targeted attacks" are low-skill attacks that target a specific firm or individual.[45] These attacks are the realm of the CFAA, Wiretap Act, and Stored Communications Act and generally involve acquaintances, employees, or romantic partners—they also generally involve scenarios where attackers have some level of access to their target's facilities and devices. Importantly, these threat actors are generally not motivated simply by a desire to access their targets' data or systems, but rather view that access as instrumental to some other purpose. Moving up from there, "Advanced Persistent Threats" ("APTs") are skilled, well-resourced, focused actors.[46] This is the realm of state-actors. APTs generally are focused on

42. *Id.* at 35.
43. *Id.*
44. *Id.*
45. BELLOVIN, *supra* note 40, at 35.
46. BELLOVIN, *supra* note 40, at 36.

valuable targets—sometimes they target a specific firm, other times they spread exploits widely to see what valuable targets they can identify.[47] Once they identify a target, they employ a sophisticated range of tools to get a foothold into the target's systems—they then slowly move laterally through the target's networks and deliberatively and carefully engage in whatever malfeasance they intend. These attacks typically go undetected for months.[48]

The reasonableness of a firm's data security is irrelevant to these first three categories of threat actors. A firm whose systems are compromised by a "Joy Hacker" has *per se* unreasonable security. Or, to state things somewhat differently, these systems' security is objectively unreasonable.[49] In the other corner of the matrix, if an APT targets a firm's systems, that APT is going to compromise them.[50] Similarly with targeted attacks – these attackers generally already have some level of access to their target's systems and the damage caused by their efforts is different in nature than that which a data security standard is intended to protect against.[51] The legal system's response to these attackers is better channeled through more specific statutes like the CFAA.

This brings us to "Opportunistic hacks" – those undertaken by skilled threat actors who do not focus on specific targets or types of targets.[52] Like Joy Hackers, these actors will compromise whatever systems they can. Like APTs they are constantly developing new tools, both to identify potential targets and to create new ways in to those targets' systems.

Opportunistic attackers are the broadest category of threats actors. They likely are the most dangerous and the most difficult category of attackers for most firms to deal with.[53] This category includes everything from ransomware to cryptojacking, from attacks designed to do nothing more than passively measure the

47. BELLOVIN, *supra* note 40, at 36.

48. *See* BELLOVIN, *supra* note 40, at 36.

49. *See infra* Section III.C.

50. *See* BELLOVIN, *supra* note 40, at 36.

51. *See* BELLOVIN, *supra* note 40, at 36.

52. *See* BELLOVIN, *supra* note 40, at 35.

53. BELLOVIN, *supra* note 40, at 35 ("Opportunistic hackers are considerably more dangerous than joy hackers … . It is likely that this class of malefactor is responsible for many of the botnets that infest the Internet today … . For many sites, the opportunistic hacker is the threat to defend against.").

"size" of the Internet to cripple it.[54] This category includes everything from phishing attacks spread randomly by e-mail, to ad-injection attacks delivered when victims go to compromised websites, and brute force scanning attacks that actively probe every IP address on the Internet looking for vulnerable targets.[55] Other categories of attackers (especially APTs) may use some of these same techniques—but opportunistic attackers deploy them indiscriminately and at scale.[56]

These attacks are also the most likely to harm consumers. Unlike APTs (generally motivated by geopolitical interests), targeted attacks (generally motivated by individualized interests), and joy hacks (generally motivated by the sheer joy of the hack), opportunistic hackers are generally interested in exploiting large numbers of systems for personal gain.[57] This may mean stealing CPU time to mine cryptocurrency, it may mean assembling massive botnets that can be sold for DDoS attacks, or it may mean stealing consumer data to sell on the dark web. These motivations mean both that Opportunistic Hackers are more likely to cause consumer harm than other types of attackers and that they have resources to invest in developing and implementing new attacks.

If there is to be a meaningful duty of data security, it should be tailored to protecting systems against Opportunistic Hackers. Unlike Bellovin's other categories of threats, the duty of data security is a lever that may meaningfully calibrate the precautions that firms take against these attackers.

B. WHAT'S THE PURPOSE OF DATA SECURITY LIABILITY?

Equipped with an understanding of the harms that a duty of data security needs to protect against, we can consider how best to use liability to protect against those harms. In the typical setting in which we impose liability on a custodian, we impose liability both for deterrent and compensatory purposes. That is, to encourage prudent investments to protect against expected harms and to compensate a harmed party for a custodian's failure to make such investment.

The basic challenge of data security is that it is unreasonably difficult for the typical firm to maintain reasonable security. As the trope goes, there are two types of firms: those that have

54. *See* BELLOVIN, *supra* note 40, at 35.
55. *See* BELLOVIN, *supra* note 40, at 35.
56. *See* BELLOVIN, *supra* note 40, at 35.
57. *See* BELLOVIN, *supra* note 40, at 35.

been breached and those that do not know that they have been breached.[58] In the adversarial setting that characterizes the data security environment, and especially one dominated by Opportunistic Hackers, maintaining security standards in proportion to the likelihood of a breach means investing up to the full value of the data likely to be compromised—over a relatively short time horizon, the likelihood of a breach approaches 100%.[59] Indeed, because this is an adversarial setting, maintaining reasonable security means keeping apace of the adversarial actors that are constantly developing new attack capabilities.

Imposing such data security obligations on all but the largest of the millions of firms that make up the American economy is an impossible burden. Internet-connected networks are an essential part of these firms' businesses. From CRM software to billing databases, accounting software and web publishing software, even simple web and e-mail access, some level of Internet connectivity is common across most of the marketplace. Each one of those systems presents a target. Just as the owner of a dry cleaner spends his days running his business, Opportunistic Hackers spend their days running theirs, looking for ways to get into that dry cleaner's computers via a phishing e-mail that silently scans hard drives for database files that may contain customer information to be silently sent back to the hackers for processing and delivery to a dark web marketplace.

Imposing an objective duty of data security on these businesses will not affect their security practices. The only thing that it will do is subject them to prospective liability should their systems be compromised and that breach detected and tied back to them. This may vindicate some carnal sense to vindictive or retributive justice; in occasional cases it may lead to compensatory damages to make a random sample of affected consumers whole; but it will not meaningfully improve the state of data security.

It should be noted that I am not, in principle, opposed to liability for data breaches. Indeed, I have written favorably about imposing strict liability for data breaches.[60] The reason for this

58. James Cook, *FBI Director: China Has Hacked Every Big US Company*, BUS. INSIDER (Oct. 6, 2014, 6:24 AM), http://www.businessinsider.com/fbi-director-china-has-hacked-every-big-us-company-2014-10 (quoting James Comey, FBI Director).

59. This discussion focuses on the probability side of the expected harm of a breach. There is a related issue about the uncertain, and highly subjective, valuation of harm that results in a breach.

60. *See, e.g.*, Justin (Gus) Hurwitz, *Cyberensuring Security*, 49 Conn. L. Rev. 1495 (2017).

is that one of the most important, but often overlooked, purposes of liability is to improve the overall quality of the data security ecosystem. That is, to make it easier to secure systems. The reality is that most firms are just as helpless as consumers, both in terms of securing their systems and in terms of improving the overall quality of the ecosystem. If we place clear liability on one cohort or the other we concentrate bargaining power in one group. This makes it more likely that that group, whichever it is, will be able to exert pressure on the firms that design software to make the security, and securability, of consumer data a higher priority. As things stand, the current approach diffuses this bargaining power, focusing consumer attention of the firms that are least able to change the status quo, and focusing those firms' attention on defending themselves against indeterminate standards.

C. WHAT'S THE STANDARD, KENNETH?

We now return to the central question: what is, or should be, the standard for a duty of data security. The standard that McGeveran has identified is one of subjective reasonableness. Did the firm invest in security in proportion to its size, complexity, resources, risk tolerance, and generally its understanding of its exposure to risk of attack?

This is a good standard.

We can reasonably impute to large firms a level of sophistication commensurate with the objective risks that they and their customers face. There is little question that a Fortune 1000 firm has access to the technical resources to understand the threat environment and to architect their systems in a way that minimizes their risk exposure.[61] The security practices of these firms can be meaningfully evaluated against the practices of their peers within the industry.

The question for smaller firms is more nuanced. In application, however, it should amount to little more than "were you trying?" Thanks in large part to the FTC's efforts in recent years, most small businesses have ample access to resources about

61. *See, e.g.,* Kenneth Bamberger & Deirdre Mulligan, *Privacy on the Books and on the Ground*, 63 STAN. L. REV. 247, 261–63 (2011) (discussing the rise of Chief Privacy Officers in U.S. firms); *but see* Hurwitz, *The FTC's Data Security Error*, *supra* note 39 (discussing an amicus brief filed in the *LabMD* case based upon Bamberger & Mulligan's article, and discussing that their research focuses exclusively on Fortune 1000 firms).

basic data security.[62] The purpose of these resources should not be—indeed, cannot be—to fully explain to a small business how to reasonably secure their systems. But these resources can meaningfully serve to make even the smallest firms aware about cybersecurity concerns in general terms and of certain threshold minimum practices. And, more important, they can educate these firms about the nature of the threats that they face. Most Americans, including those running businesses, do not have the benefit of Steve Bellovin explaining to them the threat landscape. Their mental threat model is of a Joy Hacker (or perhaps, in the modern day, an APT) trying to compromise particular systems, not of an Opportunistic Hacker attempting to compromise literally every computer on the Internet. Importantly, under this (incorrect) threat model, it makes sense for most small firms to believe that there is safety in numbers: with millions of businesses out there, most larger than me, why would any attacker single my firm out? The probability of my firm being targeted is exceptionally low, so there is little need to invest in online security.

Once small firms understand this, it becomes reasonable to ask merely whether they were putting in a good faith effort. Such a standard accomplishes most of what we can expect in terms of creating incentives for small business to invest in security. Indeed, most of the vulnerabilities that Opportunistic Hackers exploit either can be addressed with relatively minimal security investment (e.g., patching systems and changing default passwords) or cannot be avoided without significant security investment (e.g., exploitation of zero-day vulnerabilities or particularly sophisticated or targeted phishing campaigns). Importantly, by evaluating the reasonableness of the firm's conduct from a subjective perspective—asking, in effect, whether the firm was reasonably responding to its own understanding of the threat landscape—we avoid the due process issues that have dogged many efforts to develop a generally applicable duty of data security.[63]

62. In recent years, the FTC has begun to develop information for small businesses and to reach out to engage with small business around the country. *See, e.g.*, FTC, *Cybersecurity for Small Business*, https://www.ftc.gov/tips-advice/business-center/small-businesses/cybersecurity (last visited Apr. 23, 2019); FTC, *FTC to Host Cybersecurity Roundtables with Small Businesses* (July 20, 2017), https://www.ftc.gov/news-events/press-releases/2017/07/ftc-host-cybersecurity-roundtables-small-businesses ("The Federal Trade Commission is hosting small business owners in a series of public roundtables across the United States to discuss the most pressing challenges small businesses face in protecting the security of their computers and networks.").

63. See *supra*, note 25.

CONCLUSION

In the end, I don't know whether McGeveran and I agree or disagree—or, for that matter, whether he would agree with me about whether we agree or disagree. I say this in terms of both what the duty of data security is and what it should be. I overwhelmingly agree with his descriptive work resulting from his survey of the field. So much of the standard governing the duty that he identifies, however, is tailored to the specific circumstances of any given firm that it is hard to describe this standard, at its core, as anything but a subjective one, while so much of the controversy in this field has been over the FTC's efforts to develop and enforce what it seemingly characterizes as an objective standard.

A duty of data security governed by an objective standard imposes an impossible burden on most of the American economy. It exposes the millions of small businesses that make up the economy to potentially dramatic liability for risks that are largely outside of their control. Such liability is punitive bordering on vindictive, does little to create incentives for better security, and does nothing to improve the overall quality of the data and cyber security ecosystem.

A duty of data security governed by a subjective standard, on the other hand, is much more defensible. It imposes meaningful obligations on firms sophisticated enough to implement effective security programs. But it also scales well to smaller firms from which we can expect little more than good faith effort. It addresses the due process and notice concerns that have been central to many debates about the enforceability of cybersecurity duties—most notably by the FTC—in a way that preserves the core inquiry of whether a given firm was acting in a suitable way (that is, "reasonably") given that firm's own understandings of the cybersecurity ecosystem.

It was not McGeveran's intention to crystalize this aspect of the data security debate, that is, whether the duty of data security is governed by an objective or subjective standard. But he has done so, at least for how I think about these issues. By highlighting this implicit aspect of his article, I hope that this response draws attention to what I think of as the most important, if implied, contribution of his article.