2021

Cybersecurity for Idiots

Derek E. Bambauer

Article

Cybersecurity for Idiots

Derek E. Bambauer†

INTRODUCTION

Stupid is as stupid does. – Forrest Gump[1]

Regulators can improve cybersecurity by concentrating on its low-hanging fruit. For example: "solarwinds123" is self-evidently an insecure password.[2] This is particularly true for an Internet security firm named "SolarWinds." SolarWinds allowed users who knew—or guessed—that weak password to access its software updates server.[3] Worse, once logged in, users could upload files that would then be distributed to any SolarWinds client seeking the latest patch.[4] Those

† Professor of Law, University of Arizona James E. Rogers College of Law. I thank Steven Bellovin, Neil Chilson, Bryan Choi, Deven Desai, Lesley Fair, Leslie Francis, Sue Glueck, Eric Goldman, Dan Hunter, Gus Hurwitz, Kristin Johnson, Gondy Leroy, Margot Kaminski, Rotem Medzini, Thinh Nguyen, Rianna Pfefferkorn, Amelia Smith Rinehart, Alan Rozenshtein, Sharon Sandeen, Viola Schmid, Allan Sternstein, David Thaw, Charlotte Tschider, Alan Trammell, Rebecca Wexler, Felix Wu, Christopher Yoo, Tal Zarsky, the participants in the Forum Cyber at the University of Haifa, the participants in the Internet Law Works In Progress 2019 conference, the participants in the LABS colloquium at the S.J. Quinney College of Law at the University of Utah in 2020, and the participants in the 2021 Cybersecurity Law and Policy Scholars Conference for helpful suggestions and discussion. I welcome comments at <derekbambauer@email.arizona.edu>.

1. FORREST GUMP (Paramount Pictures 1994).

2. Weak, easily guessed passwords have been known security flaws for a long time, and at least since 2008. *See* FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 240 (3d Cir. 2015) (describing FTC cybersecurity enforcement action brought, in part, due to hotel chain's "use of easily guessed passwords to access the property management systems").

3. *See* Tara Seals, *The SolarWinds Perfect Storm: Default Password, Access Sales and More*, THREATPOST (Dec. 16, 2020), https://threatpost.com/solarwinds-default-password-access-sales/162327 [https://perma.cc/P8TF-VPDG]; Thomas Claburn, *We're Not Saying This Is How SolarWinds Was Backdoored, but Its FTP Password 'Leaked on GitHub in Plaintext*,' THE REGISTER (Dec. 16, 2020), https://www.theregister.com/2020/12/16/solarwinds_github_password [https://perma.cc/K65X-V3U7].

4. *See* Seals, *supra* note 3.

clients included 425 of the Fortune 500 companies,[5] along with federal government agencies such as the Departments of Commerce, Defense, Homeland Security, and the Treasury,[6] and the National Nuclear Security Administration.[7]

SolarWind's inept security practices ultimately led to a catastrophic Internet security breach—one that gave malicious attackers (probably working for the government of Russia) access to secret U.S. government systems and data, along with a huge swath of confidential information held by commercial firms.[8] Security experts have only just begun the Herculean tasks of assessing what data was compromised, which systems must be replaced, and what traps the attackers left hidden behind.[9] Thus far, the hack is known to have compromised e-mail accounts at the Department of Justice;[10] the source code for certain Microsoft programs;[11] and sealed documents filed in the federal court system,[12] among a wealth of other likely targets. A single bad apple blew up the barrel.

5. *See* Thomas P. Bossert, *I Was the Homeland Security Adviser to Trump. We're Being Hacked.*, N.Y. TIMES (Dec. 16, 2020), https://www.nytimes.com/2020/12/16/opinion/fireeye-solarwinds-russia-hack.html [https://perma.cc/UQ57-NP9D].

6. David E. Sanger & Nicole Perlroth, *More Hacking Attacks Found as Officials Warn of 'Grave Risk' to U.S. Government*, N.Y. TIMES (Dec. 17, 2020), https://www.nytimes.com/2020/12/17/us/politics/russia-cyber-hack-trump.html [https://perma.cc/2SL7-SYLZ].

7. Dan Goodin, *SolarWinds Hack That Breached Gov Networks Poses a "Grave Risk" to the Nation*, ARS TECHNICA (Dec. 17, 2020), https://arstechnica.com/information-technology/2020/12/feds-warn-that-solarwinds-hackers-likely-used-other-ways-to-breach-networks [https://perma.cc/MGF6-Y44N].

8. *See generally* Laura Hautala, *SolarWinds Hackers Accessed DHS Acting Secretary's Emails: What You Need to Know*, CNET (Mar. 29, 2021), https://www.cnet.com/news/solarwinds-hack-officially-blamed-on-russia-what-you-need-to-know [https://perma.cc/3KEN-KX27].

9. *See generally* SOLARWINDS CORP., CURRENT REPORT: FORM 8-K (Dec. 14, 2020), https://www.sec.gov/Archives/edgar/data/0001739942/000162828020017451/swi-20201214.htm [https://perma.cc/7X5M-K8UG]; Bruce Schneier, *Why Was SolarWinds So Vulnerable to a Hack?*, N.Y. TIMES (Feb. 23, 2021), https://www.nytimes.com/2021/02/23/opinion/solarwinds-hack.html [https://perma.cc/C2GE-E89F].

10. *See* Catalin Cimpanu, *SolarWinds Fallout: DOJ Says Hackers Accessed Its Microsoft O365 Email Server*, ZDNET (Jan. 6, 2021), https://www.zdnet.com/article/solarwinds-fallout-doj-says-hackers-accessed-its-microsoft-o365-email-server [https://perma.cc/VK89-P4AM].

11. *See* Ellen Nakashima, *Microsoft Says Russians Hacked Its Network, Viewing Source Code*, WASH. POST (Dec. 31, 2020), https://www.washingtonpost.com/national-security/microsoft-russian-hackers-source-coce/2020/12/31/a9b4f7cc-4b95-11eb-839a-cf4ba7b7c48c_story.html [https://perma.cc/8K4D-4K3X].

12. *See* Brian Krebs, *Sealed U.S. Court Records Exposed in SolarWinds Breach*,

Cybersecurity is difficult and complex to implement correctly, which means that cybersecurity regulation is also hard and complicated. The United States has formally specified cybersecurity as a top federal policy priority since 1997,[13] yet over two decades later, America's legal regulation of cybersecurity is a mess if not an outright disaster.[14] I argue elsewhere that this failure derives from technological timidity[15]: regulators focus on process rather than substance;[16] defer too often to the judgments of regulated entities;[17] and prefer politically palatable but practically ineffective mechanisms such as information sharing.[18] And, trend-setting enforcers such as the Federal Trade Commission tend to concentrate on amorphous holistic assessments of an organization's security rather than seeking, as an attacker would, the weak point in their systems.[19] Cybersecurity failings are persistent and pernicious.

This Essay suggests that the current parlous situation can be improved, ironically, by having regulators lower their standards. One does not need deep expertise or thorough processes to conclude that a company setting "company123" as a password has breached its security obligations.[20] I contend that concentrating regulatory attention

KREBS ON SECURITY (Jan. 7, 2021), https://krebsonsecurity.com/2021/01/sealed-u-s-court-records-exposed-in-solarwinds-breach [https://perma.cc/63VY-AJLM].

13. *See* Derek E. Bambauer, *Conundrum*, 96 MINN. L. REV. 584, 592 (2011) (discussing foundational work by President William Clinton's 1997 Commission on Critical Infrastructure Protection).

14. *See* Geneva Sands, Brian Fung, & Zachary Cohen, *Biden Administration Faces Mounting Pressure to Address SolarWinds Breach*, CNN (Jan. 23, 2021), https://www.cnn.com/2021/01/23/politics/solarwinds-hack-biden-pressure/index.html [https://perma.cc/6S8H-HG8Q].

15. *See* Derek E. Bambauer, *Ghost in the Network*, 162 U. PA. L. REV. 1011, 1038–40 (2014) [hereinafter Bambauer, *Ghost in the Network*]; Derek E. Bambauer, *Rules, Standards, and Geeks*, 5 BROOK. J. CORP. FIN. & COM. L. 49, 52–56 (2011) [hereinafter Bambauer, *Rules*].

16. *See* Bambauer, *Rules*, *supra* note 15; *see also* Bambauer, *Ghost in the Network*, *supra* note 15 at 1039–40.

17. Bambauer, *Ghosts in the Network*, *supra* note 15, at 1035–40; Bambauer, *Rules*, *supra* note 15 at 53–54.

18. *See* Derek E. Bambauer, *Sharing Shortcomings*, 47 LOY. U. CHI. L.J. 465, 484–85 (2015).

19. *See generally* Justin (Gus) Hurwitz, *Data Security and the FTC's UnCommon Law*, 101 IOWA L. REV. 955 (2016); Bambauer, *Rules*, *supra* note 15, at 53–54.

20. This has been well known for over a decade. *See* KAREN SCARFONE & MURUGIAH SOUPPAYA, NAT'L INST. STANDARDS & TECH., GUIDE TO ENTERPRISE PASSWORD MANAGEMENT (DRAFT) 3–4 (Apr. 21, 2009), https://csrc.nist.gov/csrc/media/publications/sp/800-118/archive/2009-04-21/documents/draft-sp800-118.pdf [https://perma.cc/X736-DFV9] ("Organizations should also ensure that other trivial passwords cannot be set, such as . . . the organization's name [and] simple keyboard patterns (e.g.,"qwerty",

on similarly easy cases and questions will generate a disproportionately large benefit.[21] The country needs to stringently enforce a manual of computer security's basic Defense Against the Dark Arts[22] —a "Cybersecurity for Idiots."[23] Doing so makes regulatory action easier to predict and to undertake. It helps regulators, especially generalized ones, avoid mistakes of both under and over-enforcement. This approach is especially useful for areas that are rapidly evolving in technological terms or in terms of which entities have jurisdiction to establish rules for them. And, unfortunately, terrible security practices are rampant, from hard-coded passwords[24] to unencrypted data[25] to elementary mistakes in software coding.[26]

The best way to reduce terrible security practices is for generalist regulators, like the Federal Trade Commission (FTC) and state attorneys general, to adopt an approach that is conceptually similar to tort law's negligence per se doctrine. This model has two key aspects: it establishes regulatory floors by specifying conduct that automatically generates liability, and it draws upon expertise external to the regulator to determine those floors. To be clear, the Essay does not propose employing negligence per se itself. Tort law has been largely a disappointment in addressing cybersecurity.[27] Instead, it employs

"1234!@#$")"). *See generally* William McGeveran, *The Duty of Data Security*, 103 MINN. L. REV. 1135, 1193–95 (2019) (describing security "worst practices").

21. Consider the widespread attention that the FTC's enforcement action against Wyndham, for abysmal security practices, has drawn. *See* Recent Case, FTC v. Wyndham Worldwide Corp., *799 F. 3d 236 (3d Cir. 2015)*, 129 HARV. L. REV. 1120 (Feb. 10, 2016); Hurwitz, *supra* note 19; Woodrow Hartzog & Daniel J. Solove, *The FTC as Data Security Regulator:* FTC v. Wyndham *and Its Implications*, PRIVACY & SEC. L. REP. (BNA), 13 PVLR, no. 15, Apr. 14, 2014, at 1 ("In the field of data security law, hardly any case has had as much at stake as *Federal Trade Commission v. Wyndham.*").

22. *See generally* J.K. ROWLING, HARRY POTTER AND THE CHAMBER OF SECRETS (1998).

23. Not "Cybersecurity for Dummies." "Idiots" better describes the entities committing these errors. Also, the author is not eager to court a trademark suit from the publishers of the well-known series with the other title. *See* ABOUT FOR DUMMIES, https://www.dummies.com/about-for-dummies [https://perma.cc/T7CE-EXGR].

24. *See, e.g.*, Dan Goodin, *Hard-Coded Key Vulnerability in Logix PLCs Has Severity Score of 10 out of 10*, ARS TECHNICA (Feb. 26, 2021), https://arstechnica.com/information-technology/2021/02/hard-coded-key-vulnerability-in-logix-plcs-has-severity-score-of-10-out-of-10 [https://perma.cc/B3LG-L4TL].

25. *See, e.g.*, Lily Hay Newman, *Clubhouse's Security and Privacy Lag Behind Its Explosive Growth*, WIRED (Feb. 26, 2021), https://www.wired.com/story/clubhouse-privacy-security-growth [https://perma.cc/8C3J-C8FJ].

26. *See, e.g.*, Andy Greenberg, *An Absurdly Basic Bug Let Anyone Grab All of Parler's Data*, WIRED (Jan. 12, 2021), https://www.wired.com/story/parler-hack-data-public-posts-images-video [https://perma.cc/YHN5-J9FH].

27. *See generally* Michael D. Scott, *Tort Liability for Vendors of Insecure Software: Has the Time Finally Come?*, 67 MD. L. REV. 425 (2008).

negligence per se as a helpful metaphor—a model, lens, or heuristic—to illustrate the approach that generalist regulators should take to manage cybersecurity's challenges.[28] As such, the Essay necessarily elides some of the complexities in negligence per se doctrine, concentrating instead upon its core features that make it such a useful analogy. But the proposed model is not grounded in tort; indeed, some of its more helpful aspects are at odds with tort doctrine. For example, unlike strict liability, which requires a tortfeasor to bear liability for all of the harm caused due to their conduct, the Essay's approach would impose liability when entities deviate below regulatory minima even in the absence of harm.[29] And the model is not one about rules versus standards. The distinction between the two types of legal mandates tend to collapse under scrutiny, and while cybersecurity could use more rules and fewer standards, it may be appropriate to put in place a regulatory floor that is a standard.[30] Finally, the negligence per se-style approach need not, and likely should not, displace other analytical tools for determining liability for lax cybersecurity, including for generalist regulators such as the FTC and state attorneys general. The new model will catch and weed out obvious failures, but it is unlikely to be sufficient on its own. The FTC can still engage in more nuanced negligence-style inquiries, and indeed this sort of cost-benefit analysis is built into part of its Section 5 authority.[31] The claim here is that an approach similar to negligence per se will deliver the most cost-effective benefits for generalist regulators, like the FTC, who must contend with highly constrained resources and rapidly changing technology.

This Essay does three things. First, it articulates a cybersecurity regulatory approach similar to tort's negligence per se doctrine. This

28. I thank Deven Desai, David Thaw, and Christopher Yoo for helping me elucidate this point. Yoo also offers another fascinating analogy: behavior that constitutes a per se violation of antitrust law. *See* Christopher S. Yoo, *Network Neutrality, Consumers, and Innovation*, 25 U. CHI. LEGAL F. 179, 246–47 (2008).

29. Both negligence per se and this Essay's proposal will often act like a strict liability regime, in the sense that conduct that fails to meet a given requirement will automatically result in liability. As mentioned, there are important differences among the doctrines. One is that strict liability, like negligence itself, still requires harm to manifest in most if not all cases (although market share liability can be an exception). The second is that strict liability is a set of rules internal to tort doctrine derived via judge-made common law. Negligence per se and this Essay's cybersecurity model outsource determinations for liability to other, presumably more expert entities. *See generally* Andrew Coan, *Judicial Capacity and the Substance of Constitutional Law*, 122 YALE L.J. 422 (2012).

30. *See* Bambauer, *Rules*, *supra* note 15, at 59–60.

31. *See* 15 U.S.C. § 45(n).

model is unusual in cybersecurity; it is substantive rather than procedural, and it concentrates on rules establishing minima rather than a more holistic analysis. Second, this Essay sets forth a taxonomy of regulators, and argues that the negligence per se approach is best suited to generalized enforcers confronting rapidly changing targets. Finally, it advocates for establishing this type of regulatory floor for the rapidly proliferating field of quasi-medical devices.

I. THE SECURITY REGULATOR'S LAMENT AND A NEW HOPE

Cybersecurity is notoriously hard. Those who practice in the field must make ongoing, complex, and difficult calculations about how best to protect an entity's information and systems. These challenges give attackers an advantage: defenders are always behind in time, information, and resources.[32] All of these problems create difficulties for regulators, who must both understand the underlying technology and set prescriptions that are neither too burdensome nor too scanty. These technological intricacies also provide fodder for regulatory skeptics, who suggest that information asymmetries and the lumbering pace of updates to rules mean that legal oversight will be costly at best and counterproductive at worst.[33] This position has some merit: law is notoriously poor at remaining effective yet flexible in areas of rapid technological change, such as with controls over copyrighted material[34] and new uses of pharmaceuticals.[35]

However, the better response is not for regulators to leave the field altogether—private ordering for cybersecurity has myriad structural shortcomings[36]—but instead to change their focus.[37] Rather than trying to determine when entities get cybersecurity right, regulation should concentrate on when organizations have gone badly wrong.[38]

32. *See* Derek E. Bambauer & Oliver Day, *The Hacker's Aegis*, 60 EMORY L.J. 1051, 1060–65 (2011).

33. *See, e.g.*, Hurwitz, *supra* note 19, at 1011–12. *But see* Schneier, *supra* note 9.

34. 17 U.S.C. § 1001 et seq.; *see* JESSICA LITMAN, DIGITAL COPYRIGHT 59–63 (2001); Christine C. Carlisle, *The Audio Home Recording Act of 1992*, 1 J. INTELL. PROP. L. 335, 336–38, 352 (1994); Alliance of Artists & Recording Cos. v. Denso Int'l Am., 947 F.3d 849 (D.C. Cir. 2020).

35. *See* United States v. Caronia, 703 F.3d 149, 168–69 (2d Cir. 2012); George Horvath, *Off-Label Drug Risks: Toward a New FDA Regulatory Approach*, 29 ANN. HEALTH L. 101, 115–19 (2020).

36. *See* Bambauer, *Ghost in the Network*, *supra* note 15, at 1030–36, 1040–48; Schneier, *supra* note 9. *See generally* Avery Katz, *Taking Private Ordering Seriously*, 145 U. PA. L. REV. 1745 (1996).

37. *See* David Thaw, *The Efficacy of Cybersecurity Regulation*, 30 GA. ST. U. L. REV. 287, 370–71 (2014) (advocating in favor of a mixed governance model).

38. *Cf.* McGeveran, *supra* note 20, at 1193–95.

Tort doctrine offers a helpful analogy: cybersecurity should develop a jurisprudence similar to negligence per se rather than trying to ascertain negligence.

This cybersecurity version of negligence per se will be particularly helpful to regulators with authority to police cybersecurity that is grounded in generalist terms, such as unfair competition statutes, and without the capacity to develop deep expertise in cybersecurity in a given domain. State attorneys general and the FTC, for whom cybersecurity problems are but one small aspect of a sizeable docket, are the type of regulators who might most profitably employ this approach. More specialized and expert regulators, such as the Department of Health and Human Services (which oversees enforcement of the Security Rule of the Health Insurance Portability and Accountability Act of 1996 (HIPAA)), may use enforcement models that are functionally similar to negligence per se in certain instances, but they often have enough time, personnel, and expertise to craft their own cybersecurity rules closely tailored to the needs and challenges of their sectors. HIPAA's Security Rule, for example, mandates certain security precautions regardless of whether the covered entity believes they are justified under cost-benefit analysis.[39] Other requirements are formally optional: the regulated entity does not have to adopt the precaution, but it must conduct an analysis of whether doing so is cost-justified. And if it decides against implementing the given protection, the entity must justify the decision not to do so in writing.[40] These optional requirements operate along classic negligence lines in that they are grounded in a cost-benefit calculus. The challenge for specialized regulators is that to maintain optimal efficacy, they (or Congress) must revisit their requirements through more frequent rulemaking to ensure that mandates stay current.[41] Alternatively, similar results could likely be obtained if generalized regulators could pursue liability for entities regulated by a specialist agency or entity, but only for this Essay's negligence per se style failures. The more complicated negligence-type calculus should remain the domain of specialist regulators. This hybrid model would likely be controversial, but it could reduce the transactional costs of more frequent rulemaking and might

39. *See, e.g.*, 45 C.F.R. § 164.312(a)(2)(i) (2020) (mandating that every user must have a unique identifier).

40. *See, e.g.*, 45 C.F.R. § 164.312(a)(2)(iv) (2020) (establishing data encryption as an addressable, or optional, standard).

41. Encrypting data, for example, plainly ought to be required rather than optional/addressable. *See id.* This is a prime instance of an outdated cost-benefit analysis.

be a clever way of mitigating the risk of regulatory capture for the more specialized overseers.[42]

Negligence per se for cybersecurity offers a number of advantages. It sets clear rules: this model specifies conduct that is automatically deemed a breach of the duty of care.[43] This creates a regulatory floor: entities know which choices—mistakes—lead to certain liability.[44] It offers regulated entities adequate notice of prohibited conduct. Since the negligence per se framework adopts external referents, it gives both regulators and subjects an opportunity to learn about and avoid worst practices.[45] And, negligence per se gives courts an informational advantage, since the doctrine's requirements are based on extant statutes or regulations,[46] promulgated by institutions such as legislatures or executive agencies that are likely to have greater expertise than the judicial branch.[47]

The analogy to tort doctrine is a helpful model, but it is *only* a model or a metaphor: the cybersecurity version ought to depart from its ancestor in some respects. In tort, for example, negligence per se satisfies only two of the four conditions for liability. It establishes both duty and breach, but still demands that a plaintiff show harm that is causally related to the breach.[48]

For cybersecurity, though, this approach should not require these two additional elements, for several reasons. First, the incidence of security harms far exceeds detection, or proof, of those harms.[49] Most

42. David Thaw suggests that, under certain conditions, regulatory capture may be desirable as a mechanism for revealing valuable private information held by regulated entities. *See* Thaw, *supra* note 37, at 370–71.

43. *See* RESTATEMENT (THIRD) OF TORTS: § 14 (2000).

44. *See generally* Mark A. Geistfeld, *Tort Law in the Age of Statutes*, 99 IOWA L. REV. 957, 968–83 (2014).

45. *See* McGeveran, *supra* note 20, at 1193–95. This also avoids a common complaint about the FTC's security enforcement: that it embodies an ex post facto approach constituting unfair surprise. *See* Hurwitz, *supra* note 19, at 964–66; Gerard M. Stegmaier & Wendell Bartnick, *Psychics, Russian Roulette, and Data Security: The FTC's Hidden Data Security Requirements*, 20 GEO. MASON L. REV. 673, 676 (2013).

46. *See* RESTATEMENT (THIRD) OF TORTS § 14 cmt. a (2000).

47. *See generally* Coan, *supra* note 29, at 426–32. This technique can helpfully bridge the information gap between prospective agency regulation and retrospective tort liability. *See* Kyle D. Logue, *Coordinating Sanctions in Tort*, 31 CARDOZO L. REV. 2313, 2326 (2010) ("[E]x ante agency-based regulation is considered preferable to ex post tort liability when the regulatory agency is thought to have superior (or cheaper access to) information regarding the risks of the regulated activity than does the regulated party.").

48. *See, e.g.*, Carman v. Tinkes, 762 F.3d 565, 566–68 (7th Cir. 2014).

49. *See* Sue Poremba, *Why Security Incidents Often Go Underreported*, SECURITYINTELLIGENCE (July 12, 2019), https://securityintelligence.com/articles/why-security

data breaches go unnoticed and unreported, not least because victims have pecuniary and reputational reasons not to reveal that they have been hacked.[50] Second, cybersecurity regulation is complicated by externalities: entities internalize neither the full benefit of compliance nor the full harms of breach.[51] Conditioning liability on the occurrence of damage further reduces incentives to take adequate precautions. Relatedly, cybersecurity failures have massive spillover effects.[52] The SolarWinds breach placed all of that firm's customers at risk, although only some have seen harm materialize thus far. Truly deficient security is a time bomb; it makes more sense to defuse it than to sweep up after the explosion. Finally, this approach deals with straightforward cases: the likelihood of harm depends only on the existence of a motivated attacker—precautions are inadequate by definition.[53]

Cybersecurity's negligence per se framework should also leave behind two other aspects of the tort doctrine. First, tort leavens the rule-like stringency of the per se approach by offering exemptions from liability where the defendant proffers a sufficient excuse[54] or where the victim is not in the class of persons the external rule intends to protect.[55] Neither fits well for security. Excuses are, at base, a judicial determination that the cost-benefit analysis undergirding the per se rule is inapplicable in a particular set of circumstances.[56] The cybersecurity requirements, though, are intended as substantive minima. If chosen with care, these rules should rarely run afoul of utilitarian analysis. Moreover, even if a requirement is of uncertain application to a particular defendant, the rule itself may be worth some overenforcement as a signal to other potential violators.[57] And

-incidents-often-go-underreported [https://perma.cc/Q3R9-29TX].

50. *Id.*; *see* Sasha Romanosky, David A. Hoffman, & Alessandro Acquisti, *Empirical Analysis of Data Breach Litigation*, 11 J. EMPIRICAL LEG. STUD. 74, 99–102 (2014).

51. *See* Bambauer, *Ghost in the Network*, *supra* note 15, at 1033–35; Schneier, *supra* note 9.

52. Schneier, *supra* note 9.

53. *See* Derek E. Bambauer, *Shark Tanks and Cybersecurity*, INFO/LAW (Dec. 19, 2013), https://web.archive.org/web/20180728224117/http://blogs.harvard.edu/infolaw/2013/12/19/shark-tanks-and-cybersecurity (drawing an analogy between these cybersecurity flaws and obviously dangerous physical hazards).

54. *See, e.g.*, Tedla v. Ellman, 19 N.E.2d 987, 990–91 (N.Y. 1939) (finding violation of statute likely more prudent than compliance).

55. *See, e.g.*, Haver v. Hinson, 385 So.2d 605, 608 (Miss. 1980).

56. *See generally* DOBBS' LAW OF TORTS § 156 (describing excuses as instances where "the defendant does not appear to be negligent even if he is assumed to have violated the statute").

57. This is, perhaps, a serious application of Voltaire's wry observation that "in this country it is found good, from time to time, to kill one Admiral to encourage the

most security rules are ones of general application, even if promulgated in the context of protecting specific persons. For example, the de-identified data requirements set forth by the Privacy Rule established under the auspices of HIPAA are frequently cited as relevant to debates beyond health care,[58] such as the privacy of one's movie viewing habits.[59]

This proposed model need not be the exclusive measurement of adequate security. The negligence per se approach embodies a sort of cybersecurity pessimism: it seeks to prevent worst-case scenarios. It does not need to displace more nuanced evaluations of cybersecurity compliance but offers a superior starting point.[60] By contrast, negligence is difficult and expensive to determine.[61] Its case-by-case nature has led common law courts to develop a series of doctrinal shortcuts that attempt to convert a nebulous standard into at least a few clear-cut rules. Industry custom,[62] the economic loss rule,[63] and *res ipsa loquitur*[64] are all useful though often crude mechanisms to lower the cost of adjudication and increase predictability. With negligence, a court must undertake two hard tasks—establishing the necessary level of care, and examining whether the defendant has met it—and may have to tackle a third if questions of contributory or comparative negligence arise.[65] In jurisdictions with a more economically oriented approach to tort questions, judges may need to attempt a cost-benefit analysis, weighing the likelihood and magnitude of potential harm against the expense and efficacy of precautions.[66] Though accumulated precedent serves as some guide, courts must locate the relevant

others." VOLTAIRE, CANDIDE (Philip Littell trans.) (1918).

58. *See* SIMSON L. GARFINKEL, NAT'L INST. STANDARDS & TECH, DE-IDENTIFICATION OF PERSONAL INFORMATION (Oct. 2015), https://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8053.pdf [https://perma.cc/7Y7K-4E27].

59. *See* Boris Lubarsky, *Re-Identification of "Anonymized" Data*, 1 GEO. L. TECH. REV. 202, 203 (2017).

60. *See, e.g.*, Mata v. Pacific Gas & Elec. Co., 224 Cal. App. 4th 309, 313 (Cal. Ct. App. 2014) (compliance with regulator's requirements relieved liability based on negligence per se, but not negligence).

61. See Stephen G. Gilles, *Negligence, Strict Liability, and the Cheapest Cost-Avoider*, 78 VA. L. REV. 1291, 1296 (1992).

62. *See* Gideon Parchomovsky & Alex Stein, *Torts and Innovation*, 107 MICH. L. REV. 285 (2008). *But see* The T.J. Hooper, 60 F.2d 737, 740 (2d Cir. 1932).

63. *See, e.g.*, E. River S.S. Corp. v. Transamerica Delaval, 476 U.S. 858, 873 (1986).

64. *See* RESTATEMENT (SECOND) OF TORTS § 382D (AM. L. INST. 1965).

65. *Id.* at 1296–99. This assumes that the activity should be undertaken at all, but that analysis is typically diverted by tort doctrine into strict liability.

66. *See id.*; *The T.J. Hooper*, 60 F.2d at 740.

strand within the cases and evaluate how closely the instant facts resemble it.[67]

Negligence per se for cybersecurity involves a different, simpler, and cheaper task. Its approach is intended to identify clear, certain failures rather than to resolve close cases.[68] This zone involves conduct that no reasonable person would undertake.[69] The line for reasonableness need not be fixed with complete certainty—it is enough to know that the defendant falls below it.[70] Negligence per se may have little or nothing to say about what the defendant ought to have done, but offers rich guidance on what future defendants cannot do—at least if they wish to avoid liability. It may be a close question whether a surgeon should perform an experimental procedure on an unconscious patient who faces a grave risk to her health. It is not a close call when she lets her dog do the stitching up afterwards.

The task of many cybersecurity regulators should thus be to craft a narrative of undisputed failures.[71] This will provide clear guidance on what regulated entities cannot do, or must avoid, at lower administrative cost and with less risk of error than under the holistic or negligence approach to cybersecurity precautions.[72] It also multiplies enforcement resources: one regulator's adoption of a standard promulgated by another means that both can devote attention to assessing relevant compliance.[73] A negligence per se jurisprudence will not help inform close cases, such as what a proper patch cycle should be,[74] or what steps organizations should take against zero-day attacks,

67. *See, e.g.*, Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629, 635–40 (7th Cir. 2007) (evaluating elements of a negligence claim following a data security breach); *In re* Hannaford Bros., 4 A.3d 392 (Maine 2010) (evaluating a negligence claim following the infamous Hannaford breach, in which data thieves stole up to 4.2 million debit and credit card numbers).

68. *See* Logue, *supra* note 47, at 2339 (discussing value of negligence per se model for "minimally efficient regulatory standard[s]").

69. This Essay's model contemplates clearly unreasonable conduct, of the sort that might subject the defendant to punitive damages. *See* David G. Owen, *The Moral Foundations of Punitive Damages*, 40 ALA. L. REV. 705, 730 (1989) (discussing behavior "that constitutes an extreme departure from lawful conduct").

70. *See* Logue, *supra* note 47, at 2339.

71. *See* Kevin Townsend, *Failures in Cybersecurity Fundamentals Still Primary Cause of Compromise: Report*, SEC. WK. (July 15, 2019), https://www.securityweek.com/failures-cybersecurity-fundamentals-still-primary-cause-compromise-report [https://perma.cc/7JHF-QJM2].

72. *See* Logue, *supra* note 47, at 2339.

73. *Id.* at 2340.

74. *See ECRI Update: When It Comes to Medical Device Software, Think Before You Patch*, TECHNATION (Apr. 30, 2020), https://1technation.com/ecri-update-when-it-comes-to-medical-device-software-think-before-you-patch [https://perma.cc/E7L8

but information asymmetry already makes it hard for many regulators to undertake that task effectively.[75] Enforcers can have greater effect by tackling the proverbial low-hanging fruit: looking for instances of obviously faulty cybersecurity, penalizing them, and then pursuing others in similar situations.[76]

An approach that penalizes idiots through a negligence per se-style methodology usefully narrows the set of potential malefactors that targets and regulators alike must worry about. Simple, straightforward security failures can be probed and then exploited via automated tools.[77] So, a website that is vulnerable to SQL injection attacks—like that of Sony Music Pictures in 2011—is at risk from crackers with even rudimentary skills.[78] More complex weaknesses are more likely to require greater skill to locate and compromise. The famous Stuxnet worm used to attack Iran's nuclear enrichment facilities, for example, exploited a combination of four previously unknown security weaknesses to achieve its ends—an attack of likely unprecedented sophistication.[79] Vulnerabilities, and the precautions that address them, exist along a continuum, from those that are easy to remediate to ones such as zero-day attacks that are effectively impossible to prevent.[80] Focusing on egregious failures shifts the cost calculus in three beneficial directions. First, it is cheaper for regulators to determine what precautions are minimally necessary or absolutely required, rather than establishing whether on net an entity's security measures are reasonable. Second, eliminating easy avenues of attack raises costs for hackers.[81] Finally, if attacks require more

-DVHZ].

75. *See* Bambauer, *Ghost in the Network*, *supra* note 15, at 1035–37; Schneier, *supra* note 9.

76. *See* JOHN VIEGA, THE MYTHS OF SECURITY 147 (2009) (recommending software firms "steal the low-hanging fruit from the bad guys"); Townsend, *supra* note 71.

77. *See* Townsend, *supra* note 71.

78. *See* Elinor Mills, *Hackers Taunt Sony with More Data Leaks, Hacks*, CNET (June 6, 2011), https://www.cnet.com/news/hackers-taunt-sony-with-more-data-leaks-hacks [https://perma.cc/F344-9QRM]; Adam Martin, *LulzSec's Sony Hack Really Was as Simple as It Claimed*, ATLANTIC (Sept. 22, 2011), https://www.theatlantic.com/technology/archive/2011/09/lulzsecs-sony-hack-really-was-simple-it-claimed/335527 [https://perma.cc/5LLU-QHJ2].

79. *See* Kim Zetter, *An Unprecedented Look at Stuxnet, the World's First Digital Weapon*, WIRED (Nov. 3, 2014), https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet [https://perma.cc/M4UQ-JGKT]; David Kushner, *The Real Story of Stuxnet*, IEEE SPECTRUM (Feb. 26, 2013), https://spectrum.ieee.org/the-real-story-of-stuxnet [https://perma.cc/MK96-LWWJ].

80. *See* Bambauer, *Ghost in the Network*, *supra* note 15, at 1050–52.

81. *See* VIEGA, *supra* note 76, at 79–87.

sophistication, the number of bad actors that law enforcement and others must pursue will drop, cutting costs.

This effort will be most useful if enforcers deliberately seek out examples that are basic and highly generalizable. Thus, punishing firms that use an insecure version of Linux can be useful, but it will affect relatively few actors.[82] It would be preferable to go after companies that continue to operate outdated Windows versions—something of which the U.S. government is guilty[83]—or to penalize software manufacturers that hard-code accounts or default passwords.[84] Both scenarios implicate far more actors, involve more obvious errors, and are more readily translated to other circumstances. The goal of this approach is to adopt rules that comprise regulatory minima: there is no reasonable debate that entities should take these precautions.[85] Similarly, the FTC's recent enforcement action against a dental software provider that claimed to provide HIPAA-compliant encryption, but that instead offered only a proprietary file format to protect data, offers easily recognized lessons to industry.[86] It is actually useful to crush a vendor from time to time to encourage the others to tell the truth and to use industry-standard encryption.[87]

Obvious or easily remedied security flaws are rampant in information technology. They can have dramatic consequences wholly disproportionate to the cost that would have been required to remediate them, as the SolarWinds example demonstrates. An approach modeled on negligence per se can have significant effects, especially where the relevant regulators are not technologically sophisticated, as the next Part discusses.

82. *See* Jai Vijayan, *Critical Vulnerability Patched in 'Sudo' Utility for Unix-Like OSes*, DARK READING (Jan. 27, 2021), https://www.darkreading.com/application-security/critical-vulnerability-patched-in-sudo-utility-for-unix-like-oses/d/d-id/1339996 [https://perma.cc/89DR-RJCE].

83. *See* U.S. SENATE PERMANENT SUBCOMM. ON INVESTIGATIONS, FEDERAL CYBERSECURITY: AMERICA'S DATA AT RISK 4, 16 (June 17, 2019).

84. *See* Thu T. Pham, *Hard-Coded & Default Passwords: Gateway for Massive Attacks*, DUO (July 14, 2014), https://duo.com/blog/hard-coded-and-default-passwords-massive-attacks [https://perma.cc/7TLL-EGVG].

85. *See* Logue, *supra* note 47, at 2339.

86. *See* Henry Schein Practice Solutions, Inc., No. 1423161 F.T.C. (May 26, 2013) (complaint), https://www.ftc.gov/system/files/documents/cases/160523hspscmpt.pdf [https://perma.cc/4TGU-DSTK]; Lesley Fair, *FTC Takes on Toothless Encryption Claims for Dental Practice Software*, FED TRADE COMM'N: BUS. BLOG (Jan. 5, 2016), https://www.ftc.gov/news-events/blogs/business-blog/2016/01/ftc-takes-toothless-encryption-claims-dental-practice [https://perma.cc/5T5M-YXLZ].

87. *Cf.* VOLTAIRE, *supra* note 57.

II. A TAXONOMY OF CYBERSECURITY REGULATORS

The United States, unlike many other countries, has a highly variegated system for evaluating whether an entity's cybersecurity precautions suffice—or, put differently, whether its failure to take better steps to maintain security should result in liability. This universe of regulators can be usefully organized based upon two criteria: whether the regulator is a general-purpose one or a specialized one, and whether the rate of change in the technology at issue is relatively fast or slow. The key issue that this taxonomy exposes is the information asymmetry between the enforcers and targets of regulations.[88] Regimes that involve quickly changing technologies (more applicable for Web platforms, and less so for point-of-sale terminals) or generalist regulators (who have less opportunity to develop expertise about the capabilities and challenges of the regulated) will have relatively greater gaps in understanding. The cybersecurity negligence per se model is likely to be most useful for generalized regulators dealing with fast-changing technologies, such as the Federal Trade Commission and state attorneys general in their role as security watchdog.

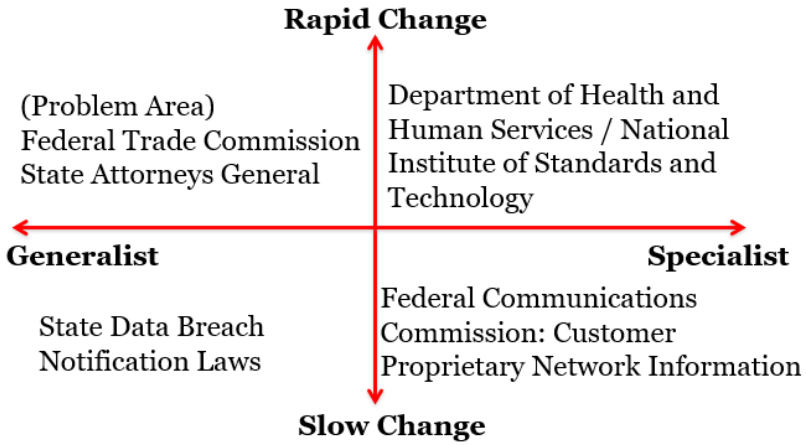

Figure 1.

A. SLOW-CHANGING TECHNOLOGY

Unsurprisingly, technologies that evolve slowly pose less of a challenge. Specialized regulators in particular can develop substantive expertise that lets them close the information gap with the entities they supervise. The Federal Communications Commission (FCC), for example, has a limited but important role in regulating consumer

88. *See* Bambauer, *Ghost in the Network*, *supra* note 15, at 1035–37.

privacy through oversight of telecommunications firms' treatment of Customer Proprietary Network Information (CPNI).[89] CPNI includes data such as the phone numbers to which a customer places calls, the duration of such calls, and value-added services that they purchase.[90] The FCC both publishes guidance on compliance[91] and enforces its rules periodically against shirkers.[92] The FCC's limited remit and its close connections with telecommunications carriers have enabled the agency to develop safeguards for CPNI that have been reasonable in terms of both benefits and burdens.[93] The Commission has staff experts on both the technology and laws involved, and CPNI has changed gradually with time—newer services such as mobile phones and Voice Over IP applications still entail management of roughly the same type of CPNI data.

Generalized regulators can also stay abreast of slow-changing technologies if the topic is sufficiently important to warrant devotion of some resources. Often, they employ generic, even all-encompassing regimes such as consumer protection statutes to police cybersecurity behavior as one type of unfair competition or deceptive practice.[94] For example, all fifty states have enacted data breach notification laws, typically enforced by the state attorney general.[95] Such requirements are likely to have low information asymmetry. These regimes are closer to rules than standards: generally, if an entity holds data containing personal information about a state's residents, and a security

89. Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information; Implementation of the Non-Accounting Safeguards of Sections 271 and 272 of the Communications Act of 1934, as Amended, 66 Fed. Reg. 50,141 (Oct. 2, 2001) (codified at 47 C.F.R. pt. 64); *see* Paul M. Schwartz, *Preemption and Privacy*, 118 YALE L. J. 902, 924 (2009); Stephen M. Ruckman & A.J.S. Dhaliwali, *The FCC's Expanding Definition of Privacy*, 19 J. INTERNET L. 1, 1 (2015). *But see* U.S. West, Inc. v. FCC, 182 F.3d 1224, 1232 (10th Cir. 1999) (invalidating requirement that carriers obtain customer approval before using CPNI for marketing purposes).

90. 47 U.S.C. § 222(h)(1).

91. *See, e.g.*, FCC ANN. CPNI CERTIFICATIONS (2011), https://docs.fcc.gov/public/attachments/DA-11-159A1.pdf [https://perma.cc/FVU7-HES2].

92. *See, e.g.*, Annual CPNI Certification: Omnibus Notice of Apparently Liability for Forfeiture and Order, FCC (Feb. 25, 2011), https://www.fcc.gov/eb/Orders/2011/DA-11-371A1.html [https://perma.cc/AU2J-8MPV].

93. *See generally* Thomas B. Norton, Note, *Internet Privacy Enforcement After Net Neutrality*, 26 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 225, 237–38 (2015).

94. *See generally* Solove & Hartzog, *supra* note 21, at 2 (describing FTC's use of broad Section 5 powers to create quasi-common law for privacy and security).

95. *See, e.g.*, ARIZ. REV. STAT. §§ 18-551, 18-552 (2018). *See generally Security Breach Notification Laws*, NAT'L CONF. ST. LEGIS. (July 17, 2020), https://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx [https://perma.cc/39DK-X8A3].

breach enables an unauthorized third party to access that data, the entity must notify those whose information was spilled.[96] The laws are not technology-dependent; liability is triggered by unauthorized access to or release of covered information stored in an information technology system, regardless of the individual characteristics of that system.[97] And, the cost-benefit calculus for data breach notifications is unlikely to shift dramatically. Notifying affected consumers will only get cheaper, benefiting entities that hold data, and risks should not change much unless adversaries improve at decrypting data or using anonymized information.[98] Detecting violations may require some expertise, but a generalized regulator can accumulate knowledge over time without necessarily mastering the technological details at issue in each case. And general-purpose regulators can exchange information, refining their rules and enforcement based on a commons of experiences.[99]

B. FAST-CHANGING TECHNOLOGY

Rapidly advancing technologies always present a challenge to regulators, particularly for those with a broad remit.[100] Specialized entities have a better chance of staying even with changes; they can focus resources on acquiring information about advances and even shaping them as they develop.[101] Cybersecurity in health care offers a pair of examples. The Department of Health and Human Services (HHS) enforces HIPAA's Security Rule for covered entities.[102] Formally, HHS implements the Security Rule through regulations promulgated under first HIPAA and then the 2013 HITECH Act that modified the original act.[103] Informally, HHS publishes quarterly newsletters that "help

96. *See, e.g.*, §§ 18-551(A), (B).

97. *Id.* at § 18-551(1) (defining "breach").

98. Advances in CPU and GPU capabilities will make decryption easier, benefiting attackers, but they also make encryption easier, benefiting defenders.

99. *See* Danielle Keats Citron, *The Privacy Policymaking of State Attorneys General*, 92 NOTRE DAME L. REV. 747, 790–95 (2016).

100. *See* Lital Helman, *Curated Innovation*, 49 AKRON L. REV. 695, 695–98 (2016).

101. The Copyright Office, for example, influences the development of technological protection measures designed to safeguard copyrighted works, as well as systems designed to bypass them. 37 C.F.R. § 201 (2021); David M. Nimmer, *A Riff on Fair Use in the Digital Millennium Copyright Act*, 148 U. PA. L. REV. 673, 681–99 (2000); Maryna Koberidze, *The DMCA Rulemaking Mechanism: Fail or Safe?*, 11 WASH. J.L. TECH. & ARTS 211, 282 (2015).

102. Specifically, HHS has delegated enforcement authority to its Office for Civil Rights. *See* Statement of Organization, Functions, and Delegations of Authority, 74 Fed. Reg. 38,663 (Aug. 4, 2009).

103. Health Insurance Reform: Security Standards, 68 Fed. Reg. 8333, 8334 (Feb.

HIPAA covered entities and business associates remain in compliance with the HIPAA Security Rule by identifying emerging or prevalent issues."[104] Since the newsletters are written by HHS's enforcement branch, they are at minimum soft law that predicts how the agency will use its authority.[105] While HHS has an array of regulatory responsibilities, it is expert in health care, and as the agency charged with transmuting HIPAA's general mandate into specific security standards, it has developed substantive expertise on cybersecurity within this industry niche.

HHS guidance on the Security Rule also draws upon research produced by the National Institute of Standards and Technology (NIST).[106] Again, formally, the NIST documents are guidance materials rather than hard law.[107] However, the two agencies have jointly held a pair of Risk Analysis Guidance Conferences, and HHS recommends the Security Rule Toolkit Application created by NIST to help organizations develop and implement compliant practices.[108] NIST is one of the most technologically adept government entities,[109] and although its guidance is frequently general purpose, the agency has focused on health care-specific cybersecurity as well.[110] The cross-pollination of

20, 2003) (codified at 45 C.F.R. 160, 162, 164); Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules; Final Rule, 78 Fed. Reg. 5565, 5566 (Jan. 25, 2013) (codified at 45 C.F.R. pts. 160, 164).

104. DEP'T HEALTH & HUMAN SERVS., SECURITY RULE GUIDANCE MATERIALS: OCR CYBER AWARENESS NEWSLETTERS (Aug. 25, 2020), https://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html [https://perma.cc/E9S5-U96L].

105. *See* Ryan Hagemann, Jennifer Huddleston Skees, & Adam Thierer, *Soft Law for Hard Problems: The Governance of Emerging Technologies in an Uncertain Future*, 17 COLO. TECH. L.J. 37, 42–46 (2018).

106. DEP'T HEALTH & HUMAN SERVS., SECURITY RULE GUIDANCE MATERIALS: NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST) SPECIAL PUBLICATIONS, https://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html [https://perma.cc/RNS3-TRUU].

107. *See* Hageman et al., *supra* note 105, at 42–46.

108. *The Security Rule*, DEP'T HEALTH & HUMAN SERVS. (Sept. 23, 2020)., https://www.hhs.gov/hipaa/for-professionals/security/index.html [https://perma.cc/S3ET-HAD6].

109. *See, e.g.*, Jeff Kosseff, *Hacking Cybersecurity*, 20 U. ILL. L. REV. 811, 822 (2020); Scott J. Shackelford, Andrew A. Proia, Brenton Martell, & Amanda N. Craig, *Toward a Global Cybersecurity Standard of Care?: Exploring the Implications of the 2014 NIST Cybersecurity Framework on Shaping Reasonable National and International Cybersecurity Practices*, 50 TEX. INT'L L.J. 305 (2015).

110. *See, e.g.*, NAT'L INST. STANDARDS & TECH., AN INTRODUCTORY RESOURCE GUIDE FOR IMPLEMENTING THE HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA) SECURITY RULE (Oct. 2008).

HHS industry expertise and NIST technological prowess creates a regulator that can maintain pace with health care cybersecurity changes.

General purpose regulators will inevitably struggle with fast-advancing technologies. The canonical cybersecurity example in the United States is the Federal Trade Commission, which has positioned itself as the country's de facto security authority.[111] Security is but a small portion of the FTC's policy portfolio: the agency is the country's premier competition regulator,[112] with responsibilities in both antitrust and consumer protection,[113] and oversees industries from funeral homes[114] to home appliances.[115] And, the FTC moved to position itself as a national privacy enforcer even before it tackled cybersecurity.[116] The agency undertakes these burdens with roughly 1100 employees.[117] Its privacy and security work has become more intensive in the last two decades. The FTC began by acting as a public enforcer of privacy and security policies promulgated by private firms but has transitioned to requiring a floor of substantive precautions in both areas regardless of what an organization promises to its consumers.[118]

For security matters, the FTC faces two key challenges. First, in at least some cases, it must determine what security measures are appropriate for a given industry (and perhaps for different-sized firms in that area).[119] Second, that determination is usually retrospective: the issue is not proper security measures when the FTC brings the case, but at the time the alleged violation occurred, which can be years earlier.[120] Legal scholars differ vociferously on how well the FTC has

111. *See* Hartzog & Solove, *supra* note 21, at 5. State attorneys general also fall in this category, particularly as California begins to develop and enforce its privacy and security statute. CAL. CIV. CODE § 1798.100 et seq.; *see* Eric Goldman, *An Introduction to the California Consumer Privacy Act (CCPA)* (July 7, 2020), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3211013 [https://perma.cc/DDG8-9DHS]. The FTC bases its cybersecurity enforcement on its capacious Section 5 powers to regulate unfair commercial practices. *See* Recent Case, *supra* note 21, at 1120.

112. *See* Hurwitz, *supra* note 21, at 999.

113. *About the FTC*, FED. TRADE COMM'N, https://www.ftc.gov/about-ftc [https://perma.cc/LN67-PPSG].

114. *See* Joshua L. Slocum, *The Funeral Rule: Where It Came From, Why It Matters, and How to Bring It to the 21st Century*, 8 WAKE FOREST J. L. & POL'Y 89, 91 (2018).

115. *See Energy Labeling Rule*, 16 C.F.R. § 305 .

116. *See* Hartzog & Solove, *supra* note 21, at 2; Hurwitz, *supra* note 19, at 967–71.

117. *See* Rory Van Loo, *The New Gatekeepers: Private Firms as Public Enforcers*, 106 VA. L. REV. 467, 510–11 (2020); Hartzog & Solove, *supra* note 21, at 601 (listing relevant divisions of Bureau of Consumer Protection and number of employees).

118. *See* Hartzog & Solove, *supra* note 21, at 599–606.

119. *See* Hurwitz, *supra* note 19, at 1003–06.

120. *Id.*; *see* FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 240–42 (3d. Cir.

attained these two goals.[121] While these tasks may become easier as the FTC develops a working "common law" of cybersecurity over time, the agency will still need to defend not just the reasonableness of its conclusions, but that they are not the result of hindsight's clarity. The cybersecurity negligence per se model reduces the effects of these challenges. Its focus on relatively uncontroversial minimal criteria reduces information costs for both tasks. And requirements that act as a floor are more likely to enjoy consensus among experts and policymakers, thus diminishing the political controversy over the FTC's agenda setting. The next Section further explores the benefits of this model for general-purpose regulators.

C. THE VIRTUES OF THE NEGLIGENCE PER SE MODEL FOR THE FTC

Of the four categories of regulators enumerated above, general-purpose ones confronted with fast-moving technologies face the greatest difficulty in establishing appropriate cybersecurity rules. This Essay's negligence per se model offers considerable benefits to enforcers like the FTC. This is particularly true because general-purpose regulators tend to have broad discretion in selecting, prosecuting, and usually settling their cases.[122] The goal of this Essay's framework is to help guide the exercise of that discretion for maximum cybersecurity benefit.[123] The cybersecurity for idiots approach will require a change of direction for the FTC. Initially, the Commission operated as a guarantor of entities' existing commitments regarding privacy and security. If, for example, an online toy company promised never to sell its customers' data, the FTC could move to enforce that pledge, even if the company itself had declared bankruptcy and the consumer information was a saleable asset for the bankruptcy trustee.[124] That role left entities subject only to other regulators and reputational pressures in crafting their policies initially—firms could abuse privacy and neglect security as much as they liked, if only they were truthful about it.

2015) (alleging security failures began in 2008, the FTC brought suit in 2012).

121. *See* Hurwitz, *supra* note 19, at 1017–18; Hartzog & Solove, *supra* note 21, at 5; Stegmaier & Bartnick, *supra* note 45, at 676.

122. *See* Hartzog & Solove, *supra* note 21, at 1–2; Hurwitz, *supra* note 19, at 957–58.

123. Thanks to Allan Sternstein for reinforcing the importance of this point, especially regarding the FTC.

124. *See* FTC v. Toysmart, No. 00-11341-RGS, 2000 WL 34016434, at *2–3 (D. Mass. July 21, 2000) (unpublished decision); Stipulation and Order Establishing Conditions on Sale of Customer Information, *In re* Toysmart.com, No. 00-13995-CJK (Bankr. E.D. Mass. July 20, 2000).

However, the Commission moved fairly quickly to impose substantive rules for both attributes.[125] That shift left the FTC vulnerable to criticism that its targets lacked notice of what the agency considered adequate security measures at any particular point in time—and, more strongly, that the Commission does not have the capabilities to arrive at such a determination in the first place.[126] The FTC's task was to defend its judgment as indicative of reasonable cybersecurity precautions—essentially, engaging in a negligence calculus. Shifting to a negligence per se approach undercuts both critiques. That model relies on information available to targets as well as enforcers about what security measures are minimally necessary, providing adequate notice. And, the Commission can draw upon outside expertise in selecting the standards it will impose under its Section 5 powers, leveraging the greater information and perhaps credibility of these sources.[127]

The cybersecurity negligence per se framework also addresses the problem of coordination for both regulators and regulated entities. Each must determine how different cybersecurity rule sets interact: if a firm complies with HIPAA's Security Rule, does it remain subject to additional requirements imposed by the FTC?[128] Lack of coordination creates several risks. First, under conditions of uncertainty, entities may feel obliged to comply with the most stringent set of regulations, effectively vitiating the less searching (but possibly more cogent) ones.[129] Second, it is possible that requirements will conflict, such that regulated entities can only choose which rules to violate, not whether to violate them at all.[130] Lastly, updates to

125. *See* Hartzog & Solove, *supra* note 21, at 1–2; Hurwitz, *supra* note 19, at 964–71.

126. *See* Hurwitz, *supra* note 19, at 1017–18; Stegmaier & Bartnick, *supra* note 45, at 720. *But see* McGeveran, *supra* note 20, at 1164 (arguing that there is emerging or emergent consensus on proper security standards).

127. *See* 15 U.S.C. § 45(a) (creating FTC's Section 5(a) enforcement authority, which allows the agency to pursue violations that involve unfair methods of competition or unfair or deceptive acts or practices). *See generally* Hartzog & Solove, *supra* note 21, at 1–2, 5; Hurwitz, *supra* note 19, at 963–80. The FTC has begun to use its Section 5 powers to impose minimum standards for protection of private information and for security precautions upon private firms.

128. *Cf.* LabMD v. FTC, 894 F.3d 1221, 1224–27 (11th Cir. 2018).

129. *See generally* Alex Raskolnikov, *Probabilistic Compliance*, 34 YALE J. ON REG. 491, 496–97 (2017).

130. One useful example derives from state anti-spam regimes in place before the federal CAN SPAM Act pre-empted most state regulations. States imposed different requirements for the subject line of unsolicited commercial e-mail messages. For example, Pennsylvania required e-mails with sexual content to begin their subject line with "ADV-ADULT", while Illinois mandated "ADV:ADLT." Compliance with both was not possible unless the sender transmitted multiple messages, each tailored to the

different regimes effectively create a constantly moving target for those subject to the rules.[131]

The coordination problem could theoretically apply to a negligence per se regime as well, but it is less likely to arise in practice. This Essay's negligence per se model is built from rules, not standards, and rules are likely to have less uncertainty than more holistic standards.[132] For the sake of simplicity, regulators could define violations as involving conduct that falls below even the most lax applicable requirements. Regulators may disagree over how complex passwords ought to be or how often they ought to be changed, but they are all likely to recognize that storing credentials in cleartext is a breach of security.[133] Different regimes do not even need to agree on substantive minima; they merely need to determine that a particular action or omission falls below each system's minimum threshold. Of course, this necessitates elucidating what those minima comprise, and then both detecting and pursuing violators, as the next Section explores.

D. EASY AND HARD CASES

In essence, this Essay argues that the FTC and other general-purpose enforcers should use their discretion in regulating cybersecurity via adjudication to take on only easy cases.[134] That depends, of course, on being able to distinguish them from the hard ones, which may be a challenge. For example, the Commission's limited staff, the relatively small number of cybersecurity actions it brings,[135] and the rapid

jurisdiction covering a particular recipient; however, determining where recipients were physically located was and is impractical. *See* Derek E. Bambauer, *Solving the Inbox Paradox: An Information-Based Policy Approach to Unsolicited E-mail Advertising*, 10 VA. J.L. & TECH. 5, 31–32, 36, 31 n.225 (2005).

131. *See* Michael P. Van Alstine, *The Costs of Legal Change*, 49 UCLA L. REV. 789, 816–22 (2002).

132. *See id.* at 822–36.

133. *See, e.g.*, Stipulated Final Order for Permanent Injunction, FTC v. Bayview Solutions, No. 1:14-cv-01830-RC (D.D.C. Apr. 21, 2015) (requiring debt brokers to implement information security precautions after they posted unencrypted consumer financial information on the Internet); McGeveran, *supra* note 20, at 1153, 1173, 1190–91 (discussing encryption as consensus requirement).

134. There are FTC enforcement actions where reasonable observers would clearly see egregious security practices. *See, e.g.*, Complaint, FTC v. Bayview Solutions, No. 1:14-CV-01830 (D.D.C. Oct. 31, 2014), https://www.ftc.gov/system/files/documents/cases/111014bayviewcmp.pdf [https://perma.cc/7LGE-7BL7] (concerning sensitive consumer financial data stored unencrypted on public web site); CBR Systems, Inc., No. C-440 F.T.C. (Apr. 29, 2013) (complaint), https://www.ftc.gov/sites/default/files/documents/cases/2013/05/130503cbrcmpt.pdf [https://perma.cc/L6GG-XKWQ] (involving financial services firm that did not encrypt backups).

135. *See* Hurwitz, *supra* note 19, at 957.

change in the state of the security art makes this a non-trivial task—as does the need to assess issues without applying the benefits of hindsight.[136] But at least that challenge is appreciably smaller than under the FTC's current model, which employs a costlier negligence approach that at times focuses on defendants whose practices, while perhaps questionable, are not self-evidently unreasonable.

For example, the Commission brought an enforcement action against, and obtained a settlement with, a Georgia auto dealership for exposing sensitive customer data through peer-to-peer (P2P) file sharing systems.[137] Firms holding such data probably should not allow P2P applications on their computers or networks. However, that is not what occurred at the Georgia dealership. The breach happened when an employee downloaded data files onto a portable flash drive to work from home.[138] The employee's home computer contained the P2P application from which the breach occurred; according to the dealership's vice president, the company's systems never had P2P software on them.[139] Thus, the real issue is the measures the car dealership ought to have put in place for employees working remotely, on

136. Encrypting the exchange of information between a user and a Web site over HTTP (using first SSL and then TLS) is one cogent example. The Electronic Frontier Foundation (EFF) launched a campaign titled "HTTPS Everywhere" to try to pressure sites to use HTTP/S. *See HTTPS Everywhere*, EFF, https://www.eff.org/https-everywhere [https://perma.cc/9CLL-2B42]. Users have been trained to look for indicators of encryption such as a green lock in the browser's location bar or the presence of the "https:" protocol indicator in the URL as signals of whether a given site adequately secures their information. Encryption was not always a cinch bet, however, particularly for sites that did not supply or demand sensitive information. Maintaining the appropriate set of certificates involved some cost and administrative overhead. More important, encrypting HTTP traffic increases the load on a server's CPU and RAM. In the period before widespread availability of relatively low-cost and high-capacity cloud computing, many organizations faced trade-offs between security and capacity that did not have obvious answers. *See, e.g.*, Mario Duarte, *Encryption Everywhere*, SNOWFLAKE, https://www.snowflake.com/blog/encryption-everywhere/ [https://perma.cc/63GH-9689] ("Data encryption, while vital, has not traditionally been within reach of all organizations primarily due to budget constraints and implementation complexity.").

137. *See* Franklin's Budget Car Sales, Inc., No. 102-3094 F.T.C. (June 12, 2012) (complaint), https://www.ftc.gov/sites/default/files/documents/cases/2012/06/120607franklinautomallcmpt.pdf [https://perma.cc/A9LX-VN73].

138. *See* Amy Wilson, *FTC, in a First, Says Georgia Dealership Failed to Safeguard Consumer Data*, AUTO. NEWS (June 13, 2012), https://www.autonews.com/article/20120613/FINANCE_AND_INSURANCE/120619934/ftc-in-a-first-says-georgia-dealership-failed-to-safeguard-consumer-data [https://perma.cc/FWG8-MRJQ].

139. *Id.*

their own devices. That question is far more complex than a straightforward prohibition on P2P software on corporate systems.

Some scholars contend that the zone of easy cases is readily determined, but perhaps not particularly large. For example, Professor Bill McGeveran discusses "worst practices" in his article arguing that data security has begun to reach a consensus on necessary precautions.[140] His article views worst practices as the inverse of best or necessary practices.[141] No sane security professional or framework, for example, would endorse keeping the default passwords initially established on a system, especially when that system is connected to public networks such as the Internet.[142] Worst practices are thus "especially egregious examples of violations."[143]

This definition of worst practices, though, is underinclusive for this Essay's purposes. The examples proffered in security frameworks are illustrative, not exhaustive. Moreover, because most of these frameworks adjust their recommendations (or demands) based upon organizational characteristics such as size and sophistication, the worst practices chosen as exemplars are likely to apply to every regulated entity, from a software company to the local dry cleaner. Egregious failures are more numerous, however. Some small organizations could reasonably decide to forgo intrusion detection software[144] or virtual private networks,[145] for example, but no bank should be able to omit two-factor authentication for online account access without liability.[146] This inevitably makes the negligence per se approach more variegated—the rules for any given entity may be clear, but regulators may need to promulgate a greater number of requirements that apply, or not, based upon an entity's industry, resources, data, and the like.[147]

A final objection is that this Essay's proposal is old news. The FTC perhaps *already* concentrates upon cybersecurity idiots, as its pattern

140. McGeveran, *supra* note 20, at 1194.

141. *Id.*

142. *Id.*

143. *Id.*

144. *See* VIEGA, *supra* note 76, at 71–74.

145. *Id.* at 213–14.

146. *See, e.g.*, Ron Lieber, *A Two-Step Plan to Stop Hackers*, N.Y. TIMES (Aug. 8, 2014), https://www.nytimes.com/2014/08/09/your-money/how-to-thwart-hackers-from-financial-accounts.html [https://perma.cc/EC7N-TSZP]; Michael P. Magrath, *NY DFS, NIST and NAIC Align on Multi-Factor Authentication in Financial Services*, CSO (Feb. 28, 2018), https://www.csoonline.com/article/3259505/ny-dfs-nist-and-naic-align-on-multi-factor-authentication-in-financial-services.html [https://perma.cc/7HLW-BNA2].

147. *See generally* Bambauer, *Rules, supra* note 15.

of enforcement actions demonstrates. Although the Commission deserves a presumption that it acts in good faith, nonetheless, this argument constitutes wishful thinking. In some instances—described above as "easy cases"—the FTC is correctly focused upon the proverbial low-hanging security fruit. In other instances, however, the Commission has intervened in situations where reasonable minds can plainly differ. Forbidding firms from installing spyware on users' computers[148] or employing default passwords[149] is uncontroversial. Dictating a process for security by design[150] or requiring firms to police employees' home computers[151] is fraught.

E. CRITIQUE AND REBUTTALS

Improving cybersecurity by focusing on idiots may seem unsatisfying. While it can drive out the worst or most incompetent actors, it does not address entities that cut corners by employing substandard but not plainly unreasonable precautions.[152] This approach also might effectively rein in generalized regulators such as the FTC and state attorneys general, who would back away from developing a doctrine of cybersecurity reasonableness to focus on a framework close to rules of ineptitude. There are several responses that, nonetheless, counsel in favor of this Essay's method.

First, general-purpose regulators in the U.S. are poorly positioned to do much more on cybersecurity, at least in terms of mandatory measures. At present, they lack resources, which means that they necessarily will lack expertise and information. The FTC brings complaints in an average of fewer than ten security cases per year.[153] The agency's staff must also meet the demands of being a national regulator for privacy, antitrust, and consumer protection more generally. In

148. *See* Sears Holdings Mgmt., No. C-4264 F.T.C. (Aug. 31, 2009) (decision and order), https://www.ftc.gov/sites/default/files/documents/cases/2009/09/090604searsdo.pdf [https://perma.cc/5H3M-C7PS]; UPromise, No. C-4351 F.T.C. (Mar. 27, 2012) (decision and order), https://www.ftc.gov/sites/default/files/documents/cases/2012/04/120403upromisedo.pdf [https://perma.cc/64A2-425F].

149. *See* FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 241 (3d. Cir. 2015).

150. *See* TRENDnet, No. C-4426 F.T.C. ¶ 8(d) (Sept. 4, 2013) (complaint), https://www.ftc.gov/sites/default/files/documents/cases/2013/09/130903trendnetcmpt.pdf [https://perma.cc/WKK9-CYJ5].

151. *See supra* notes 137–139 and accompanying text.

152. In this sense, the negligence per se cybersecurity model functions like strict liability for actors who violate the relevant rules. *Cf.* Virginia E. Nolan & Edmund Ursin, *The Revitalization of Hazardous Activity Strict Liability*, 65 N.C. L. REV. 257, 286–93 (1987); Danielle Keats Citron, *Reservoirs of Danger: The Evolution of Public and Private Law at the Dawn of the Information Age*, 80 S. CAL. L. REV. 241, 268–77 (2007).

153. *See* Hurwitz, *supra* note 19, at 957.

addition, Congress has deliberately hobbled the FTC's enforcement powers, at least relative to other executive agencies, by increasing its burden for prospective rulemaking, mandating a cost-benefit standard for certain violations, and generally depriving the agency of the ability to impose financial sanctions in the first instance.[154] While the Commission has cleverly worked around these limitations by settling most complaints,[155] that approach has vulnerabilities: a single unfavorable court decision (especially at the appellate level) could undercut the entire enforcement enterprise.[156]

Second, to the degree that the FTC is filling a gap in cybersecurity enforcement, the problem is that the gap mostly persists.[157] True remediation would require either significantly more resources for the Commission, or for Congress to put in place additional sector-specific regulators, along the lines of the Department of Health and Human Services for health care. America's current, variegated security regime tends to suggest that the second option is preferable, although the initial costs are high, and the risk of capture for specialized enforcers is ever-present.[158] Put bluntly, much of the FTC's current cybersecurity work should probably be done by more and different agencies. That prospect depends, however, on the degree to which Congress and state regulators are willing to invest resources as well as rhetoric for cybersecurity.

Third, the Commission's current reasonableness approach—in essence, a negligence test—is wrongheaded. The FTC's enforcement to date employs standards rather than rules and emphasizes procedure over substance.[159] This is backwards on both counts: cybersecurity needs more clear rules and more substantive regulation.[160] Thus, the FTC is likely providing less guidance to regulated entities than

154. *See id.* at 964–65.

155. *See id.* at 971–72.

156. *See id.* at 975–80. The LabMD case represented at least a partial setback for the FCC's efforts, at least in terms of how the agency structures the conduct it demands from a defendant when it settles a complaint. *See* LabMD v. FTC, 894 F.3d 1221 (11th Cir. 2018).

157. *See* Jeff Kosseff, *Defining Cybersecurity Law*, 103 IOWA L. REV. 985, 1011–12, 1027 (2018).

158. *See* Michael A. Livermore & Richard L. Revesz, *Regulatory Review, Capture, and Agency Inaction*, 101 GEO. L. J. 1337, 1340, 1342–44 (2013).

159. *See, e.g.*, Zoom Video Comms., No. C-4731 F.T.C. 4–7 (Jan. 19, 2021) (decision and order), https://www.ftc.gov/system/files/documents/cases/1923167_c-4731_zoom_final_order.pdf [https://perma.cc/EJG4-KNZR] (requiring Zoom to conduct series of procedural steps to evaluate its security measures).

160. *See generally* Bambauer, *Rules*, *supra* note 15, at 61–62 (elaborating these arguments).

proponents may believe.[161] Its settlement agreements are overtly flexible—target organizations are supposed to engage in and document cost-benefit analysis tailored to their size, resources, and data.[162] That makes it more difficult to second-guess regulated entities in all but egregious cases—precisely the ones that this Essay's approach concentrates upon. And, it means that any individual firm's resolution of these questions offers little guidance to competitors, and less still to organizations in other sectors.[163] Thus, a reasonableness approach risks diverting scarce resources into paperwork designed to placate the Commission. Idiocy, however, is relatively easy to diagnose and difficult to defend: even an extensive analysis on behalf of unencrypted personal data or default passwords is unlikely to persuade. The shift to driving out the worst security behaviors has the potential to offer more real-world guidance at lower cost.

III. DATA UP, CODE DOWN, AND QUASI-MEDICAL DEVICES

The advent of the Internet of Things (IoT) and the proliferation of smart wearable devices have combined to offer a useful testing ground for the cybersecurity negligence per se model. This Part explores the new world of "quasi-medical devices" and the transition of the Food and Drug Administration (FDA) from a specialized regulator to a general-purpose one. It advocates that the FDA employ the cybersecurity for idiots approach when assessing quasi-medical devices.

They may not know it, but most Americans carry a device that the Food and Drug Administration could probably regulate: a smartphone or smart watch.[164] For decades, the FDA has claimed a relatively broad remit for its oversight, but the practical and legal boundaries of the agency's enforcement authority were well-understood.[165] Vitamins and supplements were off-limits, provided their manufacturers were careful not to claim therapeutic properties for these substances.[166]

161. *See, e.g.*, Hartzog & Solove, *supra* note 20, at 585–86, 620 ("FTC privacy settlements serve as the functional equivalent to a body of common law.").

162. *See* Zoom Video Comms., No. C-4731 F.T.C. 4–7 (Jan. 19, 2021) (decision and order), https://www.ftc.gov/system/files/documents/cases/1923167_c-4731_zoom_final_order.pdf [https://perma.cc/EJG4-KNZR]; *see also* Hartzog & Solove, *supra* note 20, at 614–19.

163. Firms may also be understandably reluctant to publicize their security measures for fear of inviting attacks, or at least making attackers more likely to succeed.

164. *See* Nathan Cortez, *The Mobile Health Revolution?*, 47 U. CAL. DAVIS L. REV. 1173, 1177 (2014).

165. *See id.* at 1200–02.

166. *See* Dietary Supplement Health and Education Act of 1994, Pub. L. No. 103-

The FDA surrendered authority over cigarettes due in part to long, deliberate inaction.[167] And it opted to forego regulation of claims by products to be "natural," among other advertising boasts.[168] There was a broad consensus, though, that the agency could (and should) monitor and approve items such as prescription drugs or medical devices such as magnetic resonance imaging (MRI) machines. These specialized implements presented a classic case for regulation: significant risk of harm if misused (or, at times, properly used); information asymmetry between not only consumer and vendor, but often between physician and vendor; and little viable use outside the diagnosis and treatment of disease and illness.[169] The FDA kept certain software, such as electronic medical records databases, under its purview, but not the general purpose computers (usually PCs running the Microsoft Windows operating system) upon which the programs operated.[170]

That will change with the smartphone/watch and related devices that comprise the IoT.[171] The regulatory challenges of mobile phones

417, 108 Stat. 4325.

167. *See* FDA. v. Brown & Williamson Tobacco Corp., 529 U.S. 120, 144 (2000).

168. *See Use of the Term Natural on Food Labeling*, FDA (Oct. 22, 2018), https://www.fda.gov/food/food-labeling-nutrition/use-term-natural-food-labeling [https://perma.cc/VY3Y-CDW3]. The FDA also does not regulate claims about genetically engineered foods, for example, opting instead for suasive guidance to industry. *See, e.g.*, *Guidance for Industry: Voluntary Labeling Indicating Whether Foods Have or Have Not Been Derived from Genetically Engineered Plants*, FDA (Mar. 11, 2019), https://www.fda.gov/regulatory-information/search-fda-guidance-documents/guidance-industry-voluntary-labeling-indicating-whether-foods-have-or-have-not-been-derived [https://perma.cc/T8WR-PNR3].

169. *See generally* Matthew D. Adler, *Risk, Death and Harm: The Normative Foundations of Risk Regulation*, 87 MINN. L. REV. 1293 (2003); Kristen Underhill, *Risk-Taking and Rulemaking: Addressing Risk Compensation Behavior Through FDA Regulation of Prescription Drugs*, 30 YALE J. ON REG. 377 (2013). Put differently, few medical devices or drugs are classic "dual use" devices. Few if any people have an MRI machine for home use. By contrast, dual use devices often enable activities that are subject to regulation and others that are not. The videocassette recorder (VCR) is a famous example. *See* Sony Corp. of Am. v. Univ. City Studios, 464 U.S. 417, 419–20 (1984).

170. *See generally Clinical Decision Support Software*, FDA (Sept. 26, 2019), https://www.fda.gov/regulatory-information/search-fda-guidance-documents/clinical-decision-support-software [https://perma.cc/SS3C-ALDF].

171. There are non-digital examples of dual use devices that, at least theoretically, present the same risk. Dogs can be trained to detect cancer with a high rate of accuracy due to their acute sense of smell. African pouched rats can be taught to detect tuberculosis based on their own olfactory skills. The FDA could conceivably regulate a pet beagle used to sniff visitors to check for cancer, but it seems unlikely as a practical matter. *See Study Shows Dogs Can Accurately Sniff out Cancer in Blood*, SCI. DAILY (Apr. 8, 2019), https://www.sciencedaily.com/releases/2019/04/190408114304.htm [https://perma.cc/GS2A-U7LS]; *Giant Rats Trained to Sniff Out Tuberculosis in Africa*, NAT'L

shifted dramatically once it became sufficiently cheap to equip them with wireless radios for Internet access and high-quality cameras that made everyone a potential videographer or news reporter.[172] So, too, will the legal issues presented when fitness wristbands report wearers' heart rates to their physicians over the Internet,[173] or blood glucose monitors on the surface of the skin trigger administration of insulin via an artificial pancreas through a smartphone.[174] The technological shift leading to the advent of the IoT happened when microprocessors and Internet radios became cheap and powerful enough not only to transmit data (the upstream problem), but to receive new code and hence instructions for their devices to execute (the downstream problem). Put simply, data goes up, and code comes down. The regulatory interest is in ensuring adequate safeguards for the former such that these precautions enforce relevant privacy rules (whether set by contract or statute).[175] The interest in the latter is protecting users—both the owner of the device and others who interact with it—from unexpected or undesired behavior caused by unauthorized code running on their machines.[176]

GEOGRAPHIC (July 26, 2019), https://www.nationalgeographic.org/article/giant-rats-trained-sniff-out-tuberculosis-africa [https://perma.cc/74MJ-XXYL].

172. Consider, for example, the effects on privacy law (such as the widespread problem of burgeoning non-consensual pornography) and criminal law (such as citizen recordings of police practices, known as "cop watching"). *See, e.g.*, Danielle Keats Citron & Mary Anne Franks, *Criminalizing Revenge Porn*, 49 WAKE FOREST L. REV. 345 (2014) (discussing the rise of revenge porn with technology and evaluating practical ways to criminalize it); Jocelyn Simonson, *Copwatching*, 104 CAL. L. REV. 391 (2016) (describing how activist groups have used technology to follow and record police officers).

173. The popular Fitbit wristbands are already used to check for atrial fibrillation. Greg Licholai, *Fitbit Atrial Fibrillation Approval Revs up Competition with Apple Watch*, FORBES (Sept. 15, 2020), https://www.forbes.com/sites/greglicholai/2020/09/15/fitbit-atrial-fibrillation-approval-revs-up-competition-with-apple-watch/?sh=33af2780315c [https://perma.cc/SE9J-68EJ].

174. An open-source project named OpenAPS enables users to construct their own open-source continuous glucose monitor and insulin pump. *See* OPENAPS, https://openaps.org [https://perma.cc/B7QQ-NAKN]. Open-source software presents a fascinating challenge for regulators such as the FDA: there is no single entity responsible for its construction and maintenance, and regulating end users directly is likely to be non-viable as a political matter.

175. *See* Derek E. Bambauer, *Privacy Versus Security*, 103 J. CRIM. LAW & CRIMINOLOGY 667, 667–72 (2013).

176. *See generally* Charlotte Tschider, *Regulating the IoT: Discrimination, Privacy, and Cybersecurity in the Artificial Intelligence Age*, 96 DENVER L. REV. 87 (2018). For cybersecurity examples in medical devices, see William Alexander, *Barnaby Jack Could Hack Your Pacemaker and Make Your Heart Explode*, VICE (June 25, 2013), https://www.vice.com/en/article/avnx5j/i-worked-out-how-to-remotely-weaponise-a-pacemaker [https://perma.cc/6D79-KTG6].

There is also a sociological shift occurring. Classic medical devices such as CAT scan machines and colonoscopes are usually expensive and operated by specially trained personnel. But the lay public now has access not just to pedometers and infrared thermometers, but to increasingly sophisticated technology such as mobile ODT colposcopes[177] and air quality sensors.[178] These capabilities operate on the platform that IoT devices, such as the smartphone, offer via existing sensors and data capabilities.[179] These developments pose a regulatory conundrum for the FDA, as an increasing number of technologies move into the penumbra of its regulatory shadow.

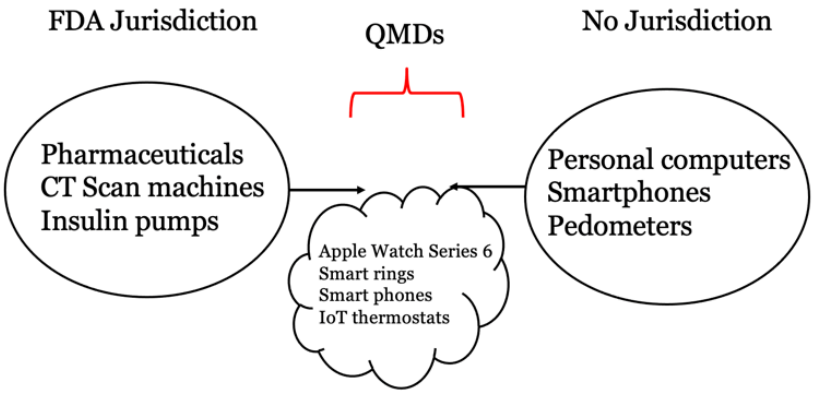

Figure 2.

The FDA will feel tempted, if not compelled, to regulate machines in the IoT if it concludes they meet the definition of a "medical device."[180] That is not a decision that is necessarily based in the agency's

177. *See* Federico Maccioni, *Beyond the Pap Smear: Startup Uses Phone, Light and AI to Detect Cervical Cancer*, TIMES OF ISR. (Jan. 21, 2019), https://www.timesofisrael.com/beyond-the-pap-smear-startup-uses-phone-light-and-ai-to-detect-cervical-cancer [https://perma.cc/BK2U-F7CP].

178. *See* Brent Rubell, *Overview: IoT Air Quality Sensor with Adafruit IO*, ADAFRUIT (Feb. 18, 2021), https://learn.adafruit.com/diy-air-quality-monitor [https://perma.cc/83XD-D98H].

179. *See generally 10 Examples of the Internet of Things in Healthcare*, ECONSULTANCY (Feb. 1, 2019), https://econsultancy.com/internet-of-things-healthcare [https://perma.cc/A457-RTS7]. Most people have experienced this type of shift, though perhaps unknowingly, when they have used wireless Internet access to place a voice phone call. To the phone and the network, voice is merely another unremarkable type of data. Put differently, "smartphone" is actually just a convenient term for a handheld computer that users often interact with using their voices.

180. *See generally* Charlotte Tschider, *Enhancing Cybersecurity for the Digital Health Marketplace*, 26 ANNALS HEALTH L. 1 (2017).

enabling statute, nor one that is necessarily wise policy. The FDA at present is a specialized regulator dealing with technologies that evolve relatively slowly. With the IoT, it will become a generalist regulator overseeing technology that changes rapidly.[181] Thus, the FDA will face tasks and challenges similar to those confronted by the FTC and state attorneys general in supervising cybersecurity. This Essay's argument is that the agency ought to choose to exercise its discretion—or be required to do so by new legislation—to treat dual use IoT devices under the negligence per se rule described above.[182] This would create a regulatory floor or minimum for items such as a Fitbit capable of detecting atrial fibrillation.[183] Technological regulation is fraught, caught between the poles of the precautionary principle and the need to generate innovation. At present, the FDA's intensive review process can actually create a barrier to cybersecurity. Although the agency maintains that most software patches that address security do not require FDA review,[184] manufacturers are wary of issuing updates because doing so may require them to undertake the certification process all over again.[185]

The FDA should adopt a variant of the famous "*Sony* safe harbor" from copyright law, which exempts dual use devices from contributory infringement liability if they are "*capable* of substantial non-infringing uses."[186] The FDA principle should be to engage in negligence per se regulation of IoT devices rather than full-fledged certification if the devices demonstrate *actual* substantial use that would subject the machines to the agency's jurisdiction, but also have *actual* substantial use that is outside the FDA's remit. This would create a new category of "quasi-medical devices," neither wholly free from oversight nor

181. *See* Helman, *supra* note 100, at 696.

182. At present, the FDA exercises discretion in deciding when to regulate machines or applications that are not clearly within or outside of the definition of a "medical device." *See* Cortez, *supra* note 164, at 1205.

183. *See* Abrar Al-Heeti, *Fitbit Launches Heart Study to See If Its Devices Can Detect AFib*, CNET NEWS (May 6, 2020), https://www.cnet.com/news/fitbit-launches-heart-study-to-explore-whether-its-devices-can-help-detect-afib [https://perma.cc/X4U3-RSPZ].

184. *See* FDA, GUIDANCE FOR INDUSTRY: CYBERSECURITY FOR NETWORKED MEDICAL DEVICES CONTAINING OFF-THE-SHELF (OTS) SOFTWARE (Jan. 14, 2005), https://www.fda.gov/media/72154/download [https://perma.cc/57ET-MWPS].

185. *See* Kristy Williams, *Updates Are Not Available: FDA Regulations Deter Manufacturers from Quickly and Effectively Responding to Software Problems Rendering Medical Devices Vulnerable to Malware and Cybersecurity Threats*, 14 WAKE FOREST J. BUS. & INTELL. PROP. L. 367, 370–71 (2014).

186. Sony Corp. of Am. v. Universal City Studios, 464 U.S. 417, 442 (1984) (emphasis added).

encumbered by lengthy evaluations that discourage innovation in both features and security.[187] For example, smartwatches with blood oxygen sensors have both medical and non-medical uses, such as evaluating the status of patients suffering from COVID[188] or aiding climbers who are exercising at altitude.[189] Regulating based upon use of the watch is infeasible, and requiring FDA approval for only the sensor component and software will, as a practical matter, hold up the development of the watch in its entirety. The negligence per se approach will help both consumers and the FDA. Consumers will be saved from devices with shoddy security measures, and the FDA can focus its resources on software and devices that are designed principally to diagnose and treat disease.[190] Thus, as the FDA enters unfamiliar terrain as a general-purpose regulator, the cybersecurity negligence per se model can help it manage these newly broadened responsibilities.

CONCLUSION

Ironically, cybersecurity regulation can become more effective if we lower our standards for its success. Specialized regulators can often cope with fast-changing technological landscapes. Generalist regulators flounder under such conditions, though they can be effective when slower advances in the state of the art keep information asymmetry to modest levels. Redefining success for generalists means shifting to a regime modeled on tort's negligence per se approach. This helps enforcement drive out obvious failure while keeping the information burden manageable for regulators. By creating a set of examples where liability is clear, regulators can create a guide to cybersecurity for idiots.

187. *See generally* Williams, *supra* note 185, at 379–99.

188. *See* Kathy Katella, *Should You Really Have a Pulse Oximeter at Home?*, YALE MED. (May 8, 2020), https://www.yalemedicine.org/news/covid-pulse-oximeter [https://perma.cc/D3L7-87RA].

189. *See* Suzana Dalul & Andy Walker, *Pulse Oximeter: What Is It and Why Does It Matter?*, ANDROID AUTH. (Feb. 9, 2021), https://www.androidauthority.com/pulse-oximeter-1068982 [https://perma.cc/CCV3-2LKG].

190. The FDA already has plenty of examples of clear cybersecurity failures, such as the use of outdated operating systems. *See, e.g.*, Heather Landi, *70% of Medical Devices Will Be Running Unsupported Windows Operating Systems by January: Report*, FIERCE HEALTHCARE (May 15, 2019), https://www.fiercehealthcare.com/tech/medical-devices-running-legacy-windows-operating-system [https://perma.cc/5RUJ-TRNB].