Marquette Intellectual Property & Innovation Law Review

Volume 26
Issue 1 *Winter*

Article 6

Winter 2022

Patching The Data Security Blanket: How A Stronger, Collaborative FTC Is The Answer Right Under Our Nose

Jose A. Gonzalez Lopez

PATCHING THE DATA SECURITY BLANKET: HOW A STRONGER, COLLABORATIVE FTC IS THE ANSWER RIGHT UNDER OUR NOSE

JOSÉ A. GONZÁLEZ LÓPEZ

I. INTRODUCTION 61
II. CURRENT PRACTICES RELATED TO THE CONSUMER PROTECTION GOAL OF DATA SECURITY 62
A. Data Breach Notification Statutes 63
B. A Common Scenario 63
C. A Glimpse of a Collaborative Enforcement Approach 64
D. Privacy Contracting 65
E. Industry Standards 66
F. Cost Efficiency 67
III. THE FTC'S ENFORCEMENT OF DATA SECURITY 67
A. The Consent Decree 68
B. The FTC as the de facto Data Police 69
C. A Comparative FTC Plan Looking Ahead 70
IV. THE PERKS AND PITFALLS OF THE FTC'S CURRENT APPROACH 72
A. Deference, does the FTC deserve any regarding its data security decisions? 73
B. Vagueness 74
C. The Vicious Cycle, Visually Represented 76
V. THE ROLE OF STATES IN PROTECTING CONSUMER DATA 77
VI. CONCLUSION 778

I. INTRODUCTION

As technology becomes more entangled with society, it becomes easier to exchange and share information. This information may take many forms across mediums, virtually encompassing any knowledge or intelligence that can be communicated between points of access.[1] Some of this information has been

1. *Information Definition*, Merriam-Webster.com Dictionary, https://www.merriam-webster.com/dictionary/information (last visited Mar. 9, 2020).

found to be protectable such as Personally Identifiable Information (PII)[2], Private Health Information (PHI)[3], financial records[4], and the GPS location from a person's cell phone.[5] Many other types of private information, however, have not received the same treatment. Protection for private information is scattered through a variety of statutes and regulations at the state level.[6]

Likewise, at the federal level, privacy protections are enforced by a number of different offices and agencies.[7] Federal laws have developed to regulate some sectors of daily life that have been deemed critical enough to warrant governmental oversight.[8] In the health context, the Health Information Portability and Accountability Act (HIPAA) filled in a need to regulate the confidentiality of the health records and information of millions of patients across the United States, where states were not already equally regulating.[9] In the financial context, the Gramm-Leach-Bliley Act (GLB) was enacted to regulate financial institutions and their practices regarding consumers' sensitive data.[10]

This Comment calls for congressional action to unify this area by expanding the statutory power of the Federal Trade Commission (FTC) in both its enforcement and rulemaking authority under the FTC Act § 5 unfair or deceptive trade practices as applied to data security. Alternatively, even if Congress does not expand the FTC's power under § 5, the agency must shift to a pre-emptive approach, providing guidance and education to entities regarding a minimum threshold of data security practices. Congressional silence in this regard must also be broken.

II. CURRENT PRACTICES RELATED TO THE CONSUMER PROTECTION GOAL OF DATA SECURITY

The consumer is the primary party of concern and who regulators seek to protect when policing data security.[11] Two primary mechanisms are after breach warnings and privacy mechanisms.

---

2. 47 U.S.C. § 551(c)(1) (2018).

3. Health Insurance Portability and Accountability Act, 45 C.F.R. § 160, 162, 164 (2021).

4. Gramm-Leach-Bliley Act, 16 C.F.R. § 314.3 (2021).

5. *See* Carpenter v. United States, 138 S. Ct. 2206 (2018).

6. Crystal N. Skelton, *FTC Data Security Enforcement: Analyzing the Past, Present, and Future*, 25 Competition: J. Anti., UCL & Priv. Section of the State Bar of Cal. 305, 305-06 (2016).

7. *See id.* at 305.

8. *Id.* at 308.

9. 45 C.F.R. § 160.203 (2021).

10. 15 U.S.C. § 6801(a) (2018).

11. F.T.C., *Privacy & Data Security Update:2019*, https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2019/2019-privacy-data-security-report-508.pdf.

A. Data Breach Notification Statutes

The most common practice linked to consumer data protection is the breach notification. A breach notification is issued by an affected entity after a breach occurs and is usually directed at customers that were affected, although at times the entire customer base is notified. Breach notification statutes exist mainly at the state level and the definitions of what falls under the statute vary slightly between each state. For example, up to the effective date of the California Consumer Privacy Act (CCPA), California's notice requirement included residents "(1) whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person, or, (2) [the information was encrypted] and the encryption key or security credential was, or is reasonably believed to have been, acquired by an unauthorized person . . . ."[12] Michigan's states that an entity must provide notice if "(a) That resident's unencrypted and unredacted personal information was accessed and acquired by an unauthorized person; or (b) That resident's personal information was accessed and acquired in encrypted form by a person with unauthorized access to the encryption key."[13] As is evident from the statutory language, there are some slight differences in the wording of both statutes where an event scenario could qualify under one, but not the other.

The problem, however, is that, in effect, issuing warnings to consumers after entities have already handed over information does not protect the consumer. Post-breach notification only allows a consumer to engage in a scramble to try to protect any other information or assets that could be compromised as a result of the original entity's breach. The breach notification is quite literally an *ex post facto* approach.

B. A Common Scenario

It is very common for simple issues, such as installing a patch for the Virtual Private Network (VPN) used by a company, to get stalled by managerial red tape or fall between the cracks of a change management process. A simple issue like that can open the window to unauthorized access and possible data breaches.

Such was the case for Equifax in 2017. After being alerted to a critical security vulnerability that affected a main production database, which handled inquiries from consumers about their personal credit data, within 48 hours

12. CA §1798.82(a).

13. [13] MI §445.72(a)–(b).

Equifax issued a request for the critical update patch to be installed.[14] Even though it would seem that all went according to plan, no one, in the chain that issued the request, double-checked to make sure that the patch was in fact installed.[15] The database went unpatched 4 months before someone at Equifax realized it, during which time multiple parties were able to gain unauthorized access to credentials that were stored in *plain text*.[16] The credentials allowed the unauthorized parties to access Social Security numbers, dates of birth, and other sensitive information; ingredients for identity theft. Notably, some of the first identified parties that were affected were those who had purchased services from Equifax, such as—wait for it—identity theft protection.[17] Aside from the overall irony of the situation, the reason this is a good example to bring up first is that you, reading this article, were potentially affected by the Equifax breach (at least 145 million Social Security numbers were stolen).

C. A Glimpse of a Collaborative Enforcement Approach

Consumer trust in Equifax was high and Equifax did act reasonably promptly to the vulnerability alert, but failing to implement "basic security measures" resulted in the company being on the wrong end of an FTC § 5 complaint and order, which it settled in 2019.[18] Equifax received penalties due to its qualifying as a financial institution under GLB, which means the Consumer Financial Protection Bureau (CFPB) was also involved in the settlement with Equifax.[19] It was a successful collaborative enforcement by the FTC and the CFPB and a proper example of how the FTC can undertake the general duties of information security while still working alongside and with existing regulation. Many scoffed at the $250 million fine imposed on Equifax, but it was a step in the right direction because it was a first instance imposition of fines because of collaboration with the CFPB.[20]

Consumers would gain more benefit if entities received guidance toward including data security as a main area of concern when designing their

14. F.T.C., *Equifax to Pay $575 Million as Part of Settlement with FTC, CFPB, and States Related to 2017 Data Breach* (July 22, 2019), https://www.ftc.gov/news-events/press-releases/2019/07/equifax-pay-575-million-part-settlement-ftc-cfpb-states-related.

15. *Id.*

16. *Id.* For context of this practice, *see* Whitson Gordon, *How Your Passwords Are Stored on the Internet (and When Your Password Strength Doesn't Matter)*, (June 20, 2012), https://lifehacker.com/how-your-passwords-are-stored-on-the-internet-and-when-5919918.

17. F.T.C., *supra* note 14.

18. F.T.C., *supra* note 14.

19. *Id.*

20. Zack Whittaker, *A year later, Equifax lost your data but faced little fallout* (Sept. 8, 2018), https://techcrunch.com/2018/09/08/equifax-one-year-later-unscathed/.

informational systems and the processes to implement/maintain them.[21] Concepts such as "Privacy by Design" have developed to help illustrate what is being asked for. When introducing Privacy by Design, Dr. Ann Cavoukian stated that moving to a Privacy by Design scheme would represent "a significant shift from traditional approaches to protecting privacy, which focus on setting out minimum standards for information management practices, and providing remedies for privacy breaches, after-the-fact."[22] The shift is significant and entails not just a change in practice, but in attitude toward the regulation of data security overall. The idea would be that data security would be part of the equation in executive and managerial decisions, and security issues would have a proper escalation channel that leads to effective decision-making and reasonably prompt responses.

While data breaches and improper exposure of data are a focal point and compose some of the more egregious examples of improper data security[23] this article argues that the overall focus must shift from the *ex post facto* approach undertaken by data privacy regulation in this present day. This is especially important in the case of the FTC, which regulates data privacy in areas not already overtaken by specific legislation.[24] The consumer engages daily with entities that may be smaller than the FTC wishes to engage with (because it is not worth the cost, which will be discussed below) and may also not be liable under other regulations or existing privacy legislation in that state. However, the affected consumer's information is gone all the same and subject to the same risks it would be if it was disclosed in a major breach or other event. It is evident, then, that this is certainly a hole in the blanket.

D. Privacy Contracting

Privacy policies are generally encouraged,[25] but at times are required.[26] The contractual nature of privacy policies lends them their importance; both agencies and courts will hold you to them, something Facebook learned the hard way. The FTC, especially, has shown that violations of a privacy policy are a deceptive practice that it will pursue.[27]

---

21. Stuart L. Pardau & Blake Edwards, *The FTC, the Unfairness Doctrine, and Privacy by Design: New Legal Frontiers in Cybersecurity*, 12 J. BUS. & TECH. L. 227, 263-64 (2017).

22. *Id.* at 264.

23. Dan Goodin, *Breach affection 1 million was caught only after hacker maxed out target's storage* (Nov. 13, 2019), https://arstechnica.com/information-technology/2019/11/breach-affecting-1-million-was-caught-only-after-hacker-maxed-out-targets-storage/.

24. Pardau, *supra* note 21, at 234.

25. WILLIAM MCGEVERAN, PRIVACY AND DATA PROTECTION LAW, 166-167 (2016).

26. *See* Gramm-Leach-Bliley Act's provision, 16 C.F.R. § 313.1 (2021).

27. *Id. see also In re* Facebook, 402 F. Supp. 3d 767 (N.D. Cal. 2019).

Privacy policies have other benefits beyond accountability that give customers the crucial confidence that much of internet commerce runs on. Writing a policy down means it can be rendered obsolete by the passing of time and technological evolution (that is good thing). Thus, policies need to be audited. This forces entities to revisit their privacy policies or face backlash from the consumers they service.[28] If that was not enough incentive, standard-setting organizations (SSO) lay out requirements for obtaining certifications that are valued by consumers.[29] These standards, in effect, increase the confidence of consumers and foster a more reliable market.[30]

E. Industry Standards

SSOs such as the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), themselves composed of a significant number of national standards bodies as members, develop and publish requirements for certified entities to adhere to.[31] For example, in the area of information security, both ISO and the IEC teamed up on the ISO/IEC 27001 standard that is widely known and followed internationally. In the United States, the National Institute of Standards and Technology (NIST), which develops its own standards, has expressly encouraged the ISO/IEC 27001 standard.[32] SSOs such as these and others like them[33] have knowledge that can only benefit an agency such as the FTC in its undertaking of the data security endeavor. Tapping experts for knowledge is not something the FTC should shy away from as long as it has the claws to assert itself as the data security martinet and the ball is in Congress's court to make that clear.[34]

---

28. *See* 16 C.F.R. § 313.1 (2021).

29. Kristen Jakobsen Osenga, *Ignorance over Innovation: Why Misunderstanding Standard Setting Organizations Will Hinder Technological Progress*, 56 U. LOUISVILLE L. REV. 159, 162, 164 (2018).

30. Timothy L. Fort & Liu Junhai, *Chinese Business and the Internet: The Infrastructure for Trust*, 35 VAND. J. TRANSNAT'L L. 1545, 1552 (2002) ("companies that state a privacy policy and abide by it, that provide and assure security for credit card transactions . . . lead to customers becoming comfortable with doing business over the Internet").

31. ISO Members List (last visted XX), https://www.iso.org/members.html.

32. NIST, *Framework for Improving Critical Infrastructure Cybersecurity* (April 16, 2018), https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

33. Institute of Electrical and Electronics Engineers (IEEE), Information Systems Audit and Control Association (ISACA)(COBIT) (last visited September 26th, 2021), https://www.ISACA.org/Resources/COBIT.

34. Justin Hurwitz, *Data Security and the FTC's UnCommon Law,* IOWA L. REV. 955, 1003 (2016).

F. Cost Efficiency

As expected, cost is a main concern. Modifying the framework in the proactive educational way proposed would require a substantial increase in expenditure up front when compared to the current scheme, which does not have such measures implemented. However, when comparing the overall cost to that of keeping regulations up to date with developing technologies, it turns out to be more cost-effective.[35] In ensuring that entities have all the education they need at the time of designing, implementing, and maintaining information security systems and processes, the FTC would enjoy a number of cost-efficiency benefits. For example, it would be much harder for an entity to deny it was on clear, fair notice and thus easier to impose fines the first time around, but the agency would need the power to do so.[36] The protection of information on the part of entities would also be more effective, quicker, and lead to less litigation as a result of improper practices.[37] Finally, the value to the consumer would be greater and, with peace of mind**,** consumers' confidence would be increased by reassurance that fewer concerns would fall through the cracks, ultimately promoting market stimulation.

III. THE FTC'S ENFORCEMENT OF DATA SECURITY

Data protection has been largely area-specific for quite some time now.[38] No real, defined inherent right to the protection of data exists, but certain areas have been determined to merit varying levels of protection.[39] In the more recent era of easy access to information, including social media and rapid gathering of personal information, the FTC has been the one to grab the reins in tackling improper data practices through its § 5 of the FTC Act, which regulates unfair or deceptive trade practices powers.[40] The FTC's § 5 power is what led to the Facebook consent decrees, the second of which included the newsworthy $5 billion fine for violating the previously agreed-upon consent decree.[41] The first

35. William McGeveran, *Friending the Privacy Regulators*, 58 ARIZ. L. REV. 959, 987–88 (2016); *see also* Julia Whall, *Policing Cyberspace: The Uncertain Future of Data Privacy and Security Enforcement in the Wake of LabMD*, 60 B.C.L. REV. E-SUPPLEMENT II.-149, II.-163 (2019).

36. *See* Hurwitz, *supra* note 34, at 1003.

37. *See* Pardau, *supra* note 21, at 274.

38. Pardau,*supra* note 21, at 274.

39. McGeveran, *supra* note 35 at 976.

40. 15 U.S.C. § 45(a).

41. Federal Trade Commission, *FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook*, (July 24, 2019), https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions.

consent decree did not involve a monetary penalty mainly because the FTC had no power to impose one.[42]

Protecting data under § 5 power has chiefly been a quasi-common law endeavor.[43] Section 5 of the FTC Act confers broad power on the FTC, but it is through both judicial and quasi-adjudicative administrative proceedings that the public is able to understand how the FTC can wield its hammer.[44] We have seen that the FTC focuses mostly on big players or events, but data breaches affecting less than 10,000 consumers have prompted FTC action under § 5.[45]

A. The Consent Decree

The FTC's preferred approach in its enforcement of §5 in the data security context has been the consent decree.[46] In part, this is likely because the consent decree is its strongest first move. The FTC cannot impose civil penalties in the data security context under § 5 unless an entity violates an already agreed-upon consent decree,[47] so tying entities to an agreement stating fines will follow upon violation is probably the best initial move when imposing §5 charges against a violating entity. Another reason is that, due to the rapid development of technology and procedural obstacles that the FTC's rulemaking authority faces, drafting regulations to cover data privacy is likely not the best alternative.[48] Still, benefits have stemmed from the FTC's approach in the pursuit of the data privacy infringer, such as opening the consumers' eyes to the data management practices of companies they engage with (such as Snapchat, Facebook, Google).

Even considering the benefits, though, the current approach is untenable. There is no doubt that the consent decree serves a purpose and that purpose heads in the general direction of protecting data. Theoretically, offering entities a first warning with instructions to follow before moving to an imposition of fines is an effective approach depending on the context. In the data security context, however, it does not quite fit the bill. There is a void and thus a need for both the FTC and entities to best ensure the consumer in society has more confidence.[49] To explore why, let us zoom out and look at the bigger picture

---

42. *See* McGeveran, *supra* note 35, at 1018.

43. Hurwitz, *supra* note 34, at 955.

44. Hurwitz, *supra* note 34 at 990.

45. LabMD, Inc. v. Fed. Trade Comm'n, 894 F.3d 1221, 1224 (11th Cir. 2018).

46. Hurwitz, *supra* note 34, at 966.

47. McGeveran, *supra* note 35, at 1019.

48. Hurwitz, *supra* note 34, at 1001; *see also* Magnuson Moss Act, Pub. L. No. 93-637, 88 Stat. 2183, 2186 (1975).

49. Thomas T. III Reith, *Consumer Confidence: the Key to Successful E-Commerce in the Global Marketplace*, 24 SUFFOLK TRANSNAT'L L. REV. 467, 486 (2001).

for a moment. Consumer confidence is a focus at both the agency and Congressional level. For example, Congress drafted the Restore Online Shoppers' Confidence Act in 2010, to be enforced by the FTC, with a provision emphasizing the importance of consumer confidence.[50] If the goal is to efficiently and effectively protect consumer data involved in activity subject to Congress's commerce-clause power, a federal governmental agency is likely the best option whose authority checks off all the elements of that goal.

B. The FTC as the de facto Data Police

In effect, the FTC seems to have become the *de facto* data security enforcer when an entity is not already overseen by one of the specifically drafted federal privacy statutes (which include statutes overseen by the Department of Health and Human Services (HHS) and the CFPB).[51] The agency can even declare an improper practice unfair or deceptive and work alongside one of the other regulating agencies like it did with Equifax.[52] This also weighs in favor of the FTC's experience, since it would surely be a larger hurdle and incur higher costs to establish a new data protection agency that has the same level of experience or rapport with coexisting agencies. Having the existing structure of an available direct appeal to federal court also provides entities the chance to argue their case to someone—having the appropriate authority—other than the FTC.[53] Courts have already shown that the deference offered to the FTC, whether interpreting its own regulations or the FTCA § 5 language itself, will not overcome generalized or vague direction from the agency.[54] Thus, entities have at least some degree of assurance in the existence of precedent showing that they have an actual shot of defending themselves.

The pivotal point is *when* privacy and data security come into consideration. Entities should be able to receive pre-emptive guidance and education when designing, building, and maintaining their information security systems and protocols. Information security integrates various practice areas including information technology, engineering, compliance and quality assurance, legal, marketing, and their respective levels of management.[55] It is important to note that regulating these areas is not to be one-sided. The idea is to spend the resources up front on education and guidance, which also promotes adherence to best practices. The concept would include an approach somewhat similar to

50. 15 U.S.C. § 8401(2) (2018).

51. Pardau, *supra* note 21, at 276.

52. F.T.C., *supra* note 14.

53. 15 U.S.C. § 45(c) (2018).

54. *See LabMD*, 894 F.3d at 1235-36.

55. Cultura Von Fun, *The Organization Module*, The Security Culture Framework (Oct. 4, 2014), https://securitycultureframework.net/the-organization-module/.

what has been termed "responsive regulation." For an extended discussion on responsive regulation and its ties to US privacy law, *see* William McGeveran, *Friending the Privacy Regulators*, 58 Ariz. L. Rev. 959, 982 (2016). Under that scheme, the regulatory agency works together with industry experts and SSOs in a role that is more partnership than antagonistic.[56] Thus, best practices would be developed in conjunction with experts and SSOs, who already engage in developing and furthering such practices.

C. A Comparative FTC Plan Looking Ahead

The plan would be for the FTC to establish its educational program including guidance materials and communication endpoints. In building up those materials, it does not even need to do most of the work, the SSOs can help with that. After all, they already do so and it is in the best interests of everyone involved that the best practices are kept up to date (especially if entities are being held to them). Some sort of committee could be created that includes the SSOs and big players to maintain the best practices with eyes to the public where the findings are published or, at the very least, subject to Freedom of Information Act requests (FOIA requests would be less preferable in the tech context due to their known delay in processing and the rapid development in this area). The responsive regulation approach, however, mainly rests on the FTC's ability to impose penalties on those it regulates.[57] With the agency not being able to back up its enforcement scheme, the scheme would effectively be brought down.[58] Yet the proposed approach, as in many cases, is predicated on people following it, so what happens when they don't?

If the idea is to promote the development of best practices and entities' adherence to such, there must be something bringing entities to the table to contribute to the discussion regarding regulation that directly applies to them. Responsive regulation rests on the "specter" of penalties being in the back of acting parties' minds.[59] The FTC must have the ability to communicate to entities that it opens the door to having a discussion, but the results will be enforced and those who do not comply will receive penalties.[60] The possibility of penalties being imposed keeps companies motivated to prioritize privacy concerns within their own structure. However, this is currently not the case, as the FTC does not have the power to impose monetary penalties on its own when

56. McGeveran, *supra* note 35, at 983-84.
57. McGeveran, *supra* note 35, at 984.
58. *See* McGeveran, *supra* note 35, at 984.
59. McGeveran, *supra* note 35, at 984.
60. McGeveran, *supra* note 35. at 985.

declaring a data security trade practice unfair or deceptive under FTCA §5 unless an entity violates an agreed-upon consent decree.[61]

Many argue that even when given the chance to impose a fine on its own, the FTC did no more than effectively slap Facebook on the wrist with the $5 billion fine it imposed.[62] Penalties as a motivator can assist, but the penalties must be up to par with the violation and the entity committing the violation, in light of the consumer.[63] In this regard, the proposed approach in this article envisions less of a "benign big-gun"[64] and does not include the all-out attack of a loss of business license included in other approaches. The public would fill in the gap by putting pressure on entities where the extreme measures of other approaches otherwise would. Both the FTC and the regulated entities can come to the table knowing that the penalties are not merely a means of the FTC swinging its hammer, but a product of society's demand for protection of its members' information. Penalties can also assist in offsetting the cost of maintaining the up-front investment on education for entities.[65]

The mention of collaboration may scare many, since initiatives in the past have involved a lot of collaboration, yet the final product was a more limited version of the original proposal.[66] Even Apple's purported limits on third-party cross-application tracking of user information were delayed at least a year after Facebook complained.[67]

The FTC's claim against Facebook under § 5, for example, involved deceptiveness regarding the company's privacy policy.[68] After its investigation, the FTC found that Facebook had "deceiv[ed] users about their ability to control the privacy of their personal information."[69] The deception was based on the company's violation of its "Statement of Rights and Responsibilities (SRR)," whose language the parties agreed was contractual.[70] Against its policy, "even after Facebook announced it would no longer give app developers access to information of users' friends, it secretly continued to give

61. McGeveran, *supra* note 35, at 1019.

62. The Editoral Board, *A $5 Billion Fine for Facebook Won't Fix Privacy*, THE NEW YORK TIMES (July 25, 2019), https://nyti.ms/2yagSvp.

63. *See* McGeveran, *supra* note 35, at 983–84.

64. McGeveran, *supra* note 35, at 984.

65. McGeveran, *supra* note 35, at 1020.

66. McGeveran, *supra* note 35, at 982.

67. Nick Statt, *Apple delays privacy feature that would let iPhone owners keep ad tracking at bay*, THE VERGE (September 3, 2020), https://www.theverge.com/2020/9/3/21420176/apple-ios-14-tracking-permission-rule-developers-delay.

68. F.T.C., *supra* note 41.

69. F.T.C., *supra* note 39.

70. *In re* Facebook, Inc., Consumer Privacy User Profile Litig., 402 F. Supp. 3d 767, 790-91 (N.D. Cal. 2019).

[third party] 'whitelisted apps' access."[71] That point hinged on whether users had consented to that activity by agreeing to the SRR and Data Use Policy, which the court found they had not.[72]

IV. THE PERKS AND PITFALLS OF THE FTC'S CURRENT APPROACH

There remains discussion to be had regarding a simple question, why should it be the FTC? The agency's experience has been discussed as a benefit and the reduced cost when compared to creating a new data protection agency has been touched on as well. However, as mentioned above, the current *ex post facto* approach hinders the overall effectiveness of the data protection scheme being enforced. The FTC also regulates data security not just through § 5 of the FTCA, but also through other regulations such as the Children's Online Privacy Protection Act (COPPA). It also oversaw the Fair Credit Reporting Act (FCRA) and the Gramm-Leach-Bliley Act (GLB) before the CFPB was around, enforcing those privacy provisions against others. The agency even has the power under some of those provisions to impose monetary civil penalties, so why not under § 5? In sum, the depth and breadth of the FTC's experience is hard to match.

However, *la vie* is not entirely *en rose* when it comes to the FTC's enforcement. A case that demonstrates some of the issues with the FTC making interpretations of regulations (in this case, it was its own) in the hopes of establishing itself as the data-privacy-police is *New York State Bar Ass'n v. F.T.C.*[73] In that case, the FTC had determined that attorneys qualified as financial institutions engaged in non-banking activities listed in GLB and, therefore, GLB's privacy provisions applied to attorneys.[74] A federal court found otherwise and held that Congress would not have intended for the FTC to regulate the ethical behavior of attorneys without explicitly saying so.[75] The outcome not only shows that the FTC can, at times, be lost at the helm, but also that Congress's silence once again plays a part. As you may have noticed and which has been discussed above, the judiciary has had to exert its power of review in determining whether the FTC is acting within its bounds in this area.

71. *Id* at 792.
72. *Id.*
73. *New York State Bar Ass'n v. F.T.C.*, 276 F. Supp. 2d 110 (D.D.C. 2003).
74. *Id.* at 111–12.
75. *Id.* at 123.

A. Deference, does the FTC deserve any regarding its data security decisions?

As was stated in *New York State Bar Ass'n*, "[a] challenge to an agency's construction of a statute that it administers is subject to the standard of review articulated in *Chevron U.S.A., Inc. v. Natural Resources Defense Council*, *Inc*., 467 U.S. 837 [] (1984)."[76] It is likely that FTC action in this context receives treatment under *Chevron* since the agency action would have the force of law and would be final unless appealed in federal court.[77] Under the *Chevron* framework, there is an initial assessment—often met in many cases—that is performed by the court to determine whether the agency had the authority to act the way it did under the implementing statute in the first place. This step is known as the preliminary "Step Zero" that precedes the *Chevron* two-step framework. In allowing the FTC to determine what constitutes an "unfair or deceptive act or practice in or affecting commerce,"[78] Congress's silence could point to an implicit delegation of authority to the FTC in making interpretations of law under its implementing statute. That is the nature of the Step Zero inquiry, which is rooted "in a theory of implicit congressional delegation of law-interpreting power to administrative agencies."[79]

There is much debate surrounding the Step Zero inquiry and has even divided justices on the Supreme Court of the United States.[80] It is important to keep in mind, however, that the issue being approached here is whether deference should be owed to the FTC's interpretation of its statute as covering data security and unfair or deceptive practices relating to data and, if deference is owed, what level of deference should be given. In approaching this question, another factor to be considered is that data security regulation is overseen by a number of agencies, as discussed here, and is not an area solely policed by the FTC. Does that then lead the FTC to receive either lower deference or none at all when making interpretations of law? Does it maybe narrow the area in which it can receive deference to its interpretations of law regarding data security? This level of uncertainty does not benefit consumers or commercial activity generally by clouding a court's route toward a proper analysis of agency action.

It could be argued that the FTC has been deemed the right agency for the job since the judiciary has at times (such as Facebook, Snapchat, etc.) upheld its injunctions and even the monetary penalties that some cases have involved.

---

76. *Id.* at 115.
77. 15 U.S.C. § 45(c) (2018).
78. 15 U.S.C. § 45(a)(1) (2018).
79. Cass R. Sunstein, *Chevron Step Zero*, 92 VA. L. REV. 187, 192 (2006).
80. *Id.*

On the other hand, it could also be argued that the judiciary has done so without any indication from Congress that this is its intent—or was its intent when granting the FTC its powers under § 5 of the FTCA—since Congress has not spoken on this point. Were that the case, the FTC could potentially be exercising its adjudicatory power outside of what was granted by Congress. That is another reason why this article calls for express congressional action in regard to the FTC and its power to enforce § 5 in the data security context. The public in general deserves more than a casual nod and an occasional affirmation by courts in this current digital age, where people's information is now in—both the literal and theoretical—cloud.

This is not to say that the Executive branch—which the FTC belongs to—requires express endorsement from Congress to exercise its quasi-legislative or quasi-judicial functions under existing statutory grants. However, as the following case demonstrates, the FTC's adjudicatory exercise in declaring data practices unfair has come under the microscope. When issuing final decision injunctions, vagueness turns out to be an issue in the resulting orders. Congressional action in granting the FTC the power to impose monetary civil fines in the first instance would better position the agency to implement the educational scheme that is being called for.

B. Vagueness

The potential limits to the FTC's current enforcement scheme were exposed in *LabMD, Inc. v. FTC*. where LabMD found itself on the wrong end of an FTC complaint and order of an injunction.[81] However, LabMD did not just roll over and challenged the FTC's order in court.[82] In that case, the medical laboratory's billing manager had installed LimeWire, a peer-to-peer file-sharing software application.[83] While using LimeWire one day, the billing manager accidentally designated the entire "My Documents" folder for sharing, which included a file containing the personal information of 9,300 customers including addresses, dates of birth, social security numbers, lab test information, and for some included health insurance information such as company and policy number.[84] This decision is relevant for a number of reasons. First, proper security practices would have easily prevented this issue. Operating systems have for over a decade included features that can limit software installations for users

81. *LabMD, Inc. v. Fed Trade Comm'n*, 894 F.3d 1221, 1227 (11th Cir. 2018).

82. *Id.* at 1226. LabMD is still the only entity to date to ever challenge (and not agree to) a consent decree in court.

83. *Id.* at 1224.

84. *Id.*

on a computer.[85] That is where the FTC's education and guidance would come into play in helping entities reach the proper understanding of how to structure their information security practices.

Second, the *LabMD* decision is a rare glimpse into the FTC's power as viewed by courts. As discussed previously, FTC §5 actions usually end in a settlement, most likely a consent decree.[86] However, LabMD stood up to the FTC's injunction and challenged it in court.[87] The decision paid off since the Eleventh Circuit vacated the order on vagueness grounds.[88] So where did the FTC go wrong with LabMD and how does that affect the spectrum of protection afforded to data? As occurs often in the practice of law, it boiled down to the text, particularly what the injunction ordered. The FTC had become accustomed to using phrases such as "reasonably designed" security programs that protect personal information.[89] The Eleventh Circuit, however, found the language to lack the requisite specificity to be enforced through any available methods.[90] The court stated that it would have been impossible for LabMD to comply with the FTC's vague standard of reasonableness without any further guidance.[91] Does that sound familiar?

The third reason is that the facts that led to the breach exemplify why it is important to have the top-to-bottom approach that this article calls for. *LabMD* is a great example of how a small thing can turn into a bigger issue because of lackadaisical approaches to information security. Did LabMD have any guidelines to follow besides some general requirement to have reasonable security measures, though? As the court explained, there was no way LabMD could have known what it had to do to comply even after the FTC issued it a direct injunction order.[92] *LabMD* also brings up another point, albeit indirectly. Entities such as LabMD may be in possession or come in contact with patient or medical information that falls under the purview of HIPAA and thus, subject to a slew of separate requirements. However, some HIPAA regulations have

85. Nathan Reynolds, *NT 4.0 System Policies VS. Win2k Group Policies,* SERVERWATCH, (Nov. 28, 2000), https://www.serverwatch.com/tutorials/article.php/2176141/NT-40-System-Policies-VS-Win2k-Group-Policies.html.

86. Hurwitz, *supra* note 34, at 966.

87. *LabMD*, 894 F.3d at 1226.

88. *Id.* at 1237.

89. Julia Whall, *Policing Cyberspace: The Uncertain Future of Data Privacy and Security Enforcement in the Wake of LabMD*, 60 B.C.L. REV. E-SUPPLEMENT II. 149, 158 (2019).

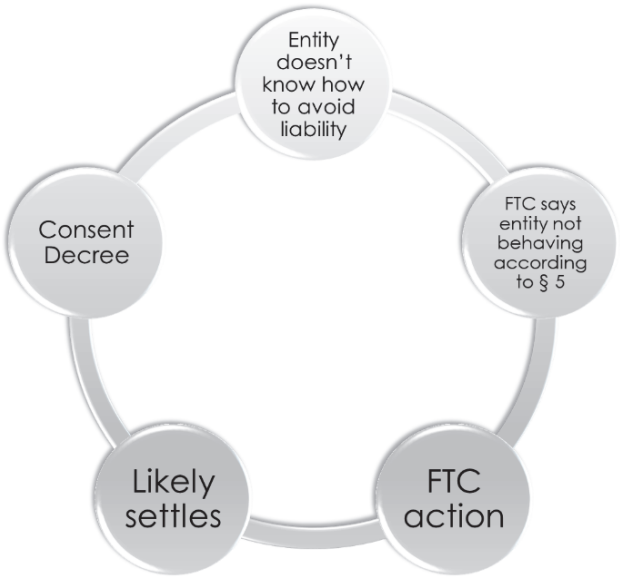
90. *Id.* at 158–59.

91. *Id.* at 158.

92. *Id.*

similarly ambiguous language to the FTC's reasonableness standard.[93,94] The difference is the Department of Health and Human Services can impose civil penalties on those that violate its regulations.[95] Nevertheless, all governmental agencies that enforce any kind of information security regulations can benefit from an education-first approach to such enforcement (some more than others because they have the "specter" of civil penalties keeping entities in check).

C. The Vicious Cycle, Visually Represented



Current approach

One of the dangers of the FTC's current *ex post facto* approach is that, in effect, it turns out to be quite cyclical. The usual scenarios begin with the FTC finding that an entity has violated FTCA § 5 in some way, shape, or form.[96] The graphic above does not make the distinction of where the cycle usually begins because no matter where you are in the cycle, the enforcement framework brings you right back around the circle with no theoretical end in sight.

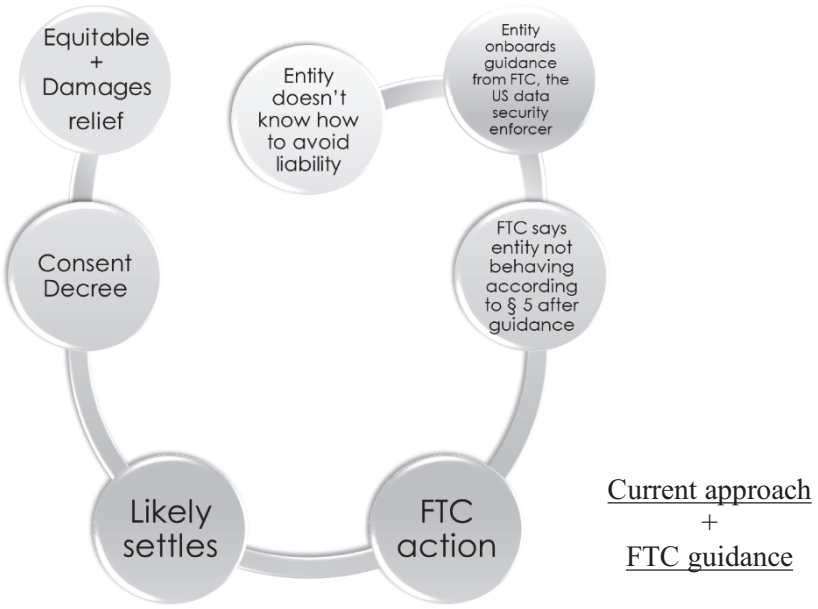
---

93. Sharona Hoffman & Andy Podgurski, *In Sickness, Health, and Cyberspace: Protecting the Security of Electronic Private Health Information*, 48 B.C. L. REV. 331, 372 (2007).

94. Such is the case with the Gramm-Leach-Bliley Act as well. 16 C.F.R. § 314.3 (2021).

95. Hoffman, *supra* note 93, at 342

96. Skelton, *supra* note 6, at 306.



As opposed to other approaches that discourage minimum thresholds for their fixation,[97] the proposed approach in this article envisions a minimum threshold of responsibility that attaches to entities once the FTC can cement its status as the data security resource/enforcer. With the availability of the FTC and its educational and guidance resources, notice would be received at an earlier time of entities' development. Collaboration with states can assist in this sense. Distribution and a wider reach of communication would help spread the knowledge quicker and more efficiently.

V. THE ROLE OF STATES IN PROTECTING CONSUMER DATA

States also play a role in the protection of their residents' information through oversight and state statutes that, in some cases, have the requisite authority to impose penalties and have done so definitively. For example, California imposed a $33 million penalty on Comcast for making money from unauthorized disclosure of unlisted or unpublished phone numbers, including $25 million in civil penalties that Comcast voluntarily settled.[98] However, the fact that (outside the health and education sectors) many states have only implemented data breach notification statutes exemplifies the fact that the current dynamic only comes into play after the fact if the FTC or the state do

97. Pardau, *supra* note 21, at 264.

98. *Cal. v. Comcast Cable Commc'n. Mgmt., LLC,* Case No. 15786197 (Cal. Superior Ct, Alameda County, Sept. 17, 2015).

not get involved.[99] States' role in the data protection scheme brings up notions of federalism that are outside the scope of this article, but it bears mentioning that the proposed approach includes the FTC working alongside states (or their attorney general) and their own privacy regulations that may be even stricter than their federal equivalent.

Nevertheless, the lack of uniformity in data security regulation plagues the state level as well. To give an example, on March 9th, 2020, HHS finalized a set of proposed regulations to offer patients more access to and control over their data.[100] There has been some discussion regarding the proposed rule because some of its provisions seemed to conflict with HIPAA and state regulations.[101] The focus, then, shifts to "[e]nsuring those rules work in concert as states also set their own standards[, which] will be critical to keeping patient data secure. . . ."[102] To add to the hodge-podge, as of the beginning of 2020 at least eight states had inserted their own patient protections into their health data standards.[103] Unsurprisingly, the state frameworks would all end up being slightly different, which can lead to major headaches on the compliance side.[104] Although involving HHS and being directly under the medical information category, this example is illuminative because the call for uniformity in detail also applies to the FTC's approach under § 5.[105] Uniformity may not be favorable in approaching enforcement,[106] but knowing entities are on the same level of notice as to applicable regulation and what it requires can certainly offer a clearer picture.

VI. CONCLUSION

In the end, this endeavor is meant to benefit everyone involved by ensuring better protection of consumers' information. Society mandates a more collaborative environment than what we have seen of information security enforcement in recent past. As the FTC engages in more amicable, inclusive dialogue with SSOs and entities, the improvement will be readily observable.

---

99. William McGerveran, *The Duty of Data Security*, 103 MINN. L. REV. 1135, 1152 (2019).

100. Department of Health and Human Services, *HHS Finalizes Historic Rules to Provide Patients More Control of Their Health Data* (Mar. 9, 2020), https://www.hhs.gov/about/news/2020/03/09/hhs-finalizes-historic-rules-to-provide-patients-more-control-of-their-health-data.html.

101. Ayanna Alexander, *Busy Privacy Agenda for 2020 Has Health Companies on Edge* (Dec. 31, 2019), https://www.bloomberglaw.com/product/blaw/document/X8F4C2G0000000?.

102. *Id.*

103. *Id.*

104. *Id.*

105. Hurwitz, *supra* note 34, at 997.

106. Woodrow Hartzog & Daniel J. Solove, *The Scope and Potential of FTC Data Protection*, 83 GEO. WASH. L. REV. 2230, 2234 (2015).