Free markets. Real solutions.

R STREET POLICY STUDY NO. 116
October 2017

RESOLVING CYBERSECURITY JURISDICTION BETWEEN THE FTC AND FCC

Tom Struble

CONTENTS

INTRODUCTION

Cybersecurity has never been more important. The proliferation of digital services and connected devices, and the concomitant spread of personal information, has generated tremendous benefits for consumers and the economy. However, it has also fed a growing body of hackers and criminal enterprises who seek to profit by exploiting cybersecurity vulnerabilities in either the storage or transmission of sensitive data.[1] Moreover, given our increasing reliance on digital technologies and services, even mere human error in cybersecurity practices can now cost real human lives.[2]

While market forces can discipline cybersecurity practices to some degree,[3] government regulation will likely still be necessary to ensure that certain areas, like emergency services, maintain adequate cybersecurity. Additionally, given the complex nature of cybersecurity and the difficulties many consumers have in understanding how to value security against other factors — like privacy, convenience and cost[4] — the impact of market forces may be limited in this area, and government regulation may be necessary in order to protect consumers or competition from harmful practices, at least until the nascent cyber-insurance industry gets off the ground.[5]

Of course, the cybersecurity practices maintained by the U.S. government are vitally important today, both in the context of data breaches[6] and cyberattacks.[7] However, the present study focuses on practices currently employed in the private sector, such as those maintained by broadband providers, websites, applications and other private actors in the internet ecosystem. Such commercial cybersecurity practices are overseen by the Federal Trade Commission (FTC), sometimes in coordination with sector-specific agencies like the Securities and Exchange Commission (SEC), the Department of Health and Human Services (HHS) and the Federal Communications Commission (FCC). While the FTC's coordination with the SEC and HHS is generally well-defined, coordination between the FTC and FCC has

1. See, e.g., Sheizaf Rafaeli & Daphne R. Raban, "Information Sharing Online: A Research Challenge," *Int'l Journal of Knowledge & Learning* 62:1 (2005). https://goo.gl/M6Ud1n; Dan Patterson, "Experts Predict 2017's Biggest Cybersecurity Threats," TechRepublic, Dec. 13, 2016. https://goo.gl/XAb3Zs.

2. See, e.g., Ryan Knutson, "FCC Cracking Down on 911 Service Failures," *The Wall Street Journal*, July 17, 2015. https://goo.gl/QqPMBC.

3. See, e.g., Scott Dynes et al., "Cyber Security: Are Economic Incentives Adequate?" in *Critical Infrastructure Protection* 253, eds. E. Goetz and S. Shenoi (Boston: Springer, 2008), pp. 15, 24. https://goo.gl/qCqbPf.

4. See, e.g., Rob Van den Dam, "Sharing Personal Data vs. Privacy? The Tradeoffs of Giving Your Info to CSPs," Forbes, Feb. 27, 2017. https://goo.gl/SgB89L.

5. See, e.g., Ian Adams, "The Promise and Limits of Private Cyber Insurance," *R Street Policy Study* No. 78, December 2016. https://goo.gl/JTmpui.

6. See, e.g., Kim Zetter & Andy Greenberg, "Why the OPM Breach is Such a Security and Privacy Debacle," Wired, June 11, 2015. https://goo.gl/5CraAt.

7. See, e.g., Dustin Volz & Jim Finkle, "U.S. Blames North Korean Government for Cyber Attacks Since 2009," Reuters, June 13, 2017. https://goo.gl/3kpF4g.

been rendered murky by jurisdictional turf wars and shifting responsibilities between the two agencies.[8]

The FTC is a general-purpose competition and consumer-protection agency, with broad jurisdiction, flexible legal standards, multiple enforcement tools and substantial experience regulating commercial cybersecurity practices. By contrast, the FCC is a sector-specific agency charged with regulating the communications industry. Compared to the FTC, the FCC's jurisdiction is more limited, as are its enforcement tools, but it has more experience regulating cybersecurity in certain areas, and it has the authority to supplement its flexible legal standards with more specific rules. On balance, the FTC is better suited to regulate commercial cybersecurity practices, and ideally it would handle as much of that task as possible. However, given the overlap between the scope and expertise of the two agencies, the FCC also has a key role to play. For this reason, it is of the utmost importance for these roles to be clearly defined and for each agency to know precisely what responsibilities it has in order to avoid regulatory conflicts.

There are multiple options for how roles and responsibilities for commercial cybersecurity regulation could be divided between the FTC and FCC. For example, responsibilities could be divided based upon whether the data in question is "at rest" or "in transit."[9] Alternatively, the FCC could regulate the cybersecurity of all "common carriers," while the FTC regulates everyone else. However, the most logical division of responsibilities is for the FCC to regulate the cybersecurity of all "common-carrier services," including emergency services, while the FTC regulates all other commercial cybersecurity practices. This division could be achieved within existing law, but it may be advisable for Congress to step in and cement these roles via legislation.

CYBERSECURITY REGULATION AT THE FTC

The FTC is a general-purpose competition and consumer-protection agency, with broad jurisdiction, flexible legal standards, multiple enforcement tools and substantial experience in regulating commercial cybersecurity practices.[10] It is relatively well-suited to cybersecurity regulation, and it has substantial experience in the area, with several notable feathers in its enforcement cap, as well as an internet ecosystem that has been thriving under its watch.[11]

There is certainly much that could be improved about the FTC's investigatory processes, the use of its enforcement authority and its jurisdictional limits,[12] but when it comes to commercial cybersecurity regulation, the agency remains the most qualified federal agency in the United States. For this reason, it would be ideal for it to handle all commercial cybersecurity regulation, or as close to all of it as possible, in order to ensure consistency in both standards and enforcement throughout the internet ecosystem.

Jurisdictional scope

The FTC administers the Federal Trade Commission Act,[13] which includes general authority to police "unfair methods of competition"[14] and "unfair or deceptive acts or practices"[15] on a case-by-case basis,[16] as well as several limited grants of rulemaking authority to cover specific areas of particular concern, like credit reporting,[17] health information[18] and children's advertising.[19] Its jurisdiction is broad, but limited by several specific exclusions in Section 5(a)(2), including, notably, "common carriers subject to the Acts to regulate commerce," which includes Title II of the Communications Act.[20]

This limitation on the FTC's jurisdiction, generally referred to as the "common-carrier exemption," historically has meant that telephony services — as common-carrier services covered under Title II of the Communications Act — were outside the FTC's jurisdiction and could only be regulated by the FCC. However, in early 2015, the common-carrier exemption grew in scope when the FCC reclassified broadband internet access service ("broadband") under Title II of the Communications Act.[21] This stripped the FTC of its authority to regulate such services.

8. See, e.g., David Hatch, "FCC Sparks Turf Wars as it Raises Washington Profile," *Forbes*, March 31, 2016. https://goo.gl/UuL3od.

9. Data in transit is moving actively across a network, such as the internet. Data at rest is stored on a device or in some other media, but not transiting a network.

10. U.S. Federal Trade Commission, "About the FTC," 2017. https://goo.gl/orNQJt.

11. U.S. Federal Trade Commission, "Data Security," 2017. https://goo.gl/ThXRNd.

12. See, e.g., Berin Szóka and Graham Owens, "FTC Stakeholder Perspectives: Reform Proposals to Improve Fairness, Innovation, and Consumer Welfare," *Testimony of TechFreedom before the Subcommittee on Consumer Protection, Product Safety, Insurance & Data Security of the U.S. Senate Committee on Commerce, Science & Transportation*, Sept. 26, 2017. https://goo.gl/tN9xKR.

13. U.S. Federal Trade Commission Act, Pub. L. No. 63-311, 38 Stat. 717 (1914) (codified as amended at 15 U.S.C. 41 et seq.).

14. Ibid., § 5, 38 Stat. 719.

15. Wheeler-Lea Act, ch. 49, § 3, 52 Stat. 111 (1938) (codified at 15 U.S.C. § 45(a)(1)).

16. Federal Trade Commission Improvements Act of 1980, Pub. L. No. 96-252, 94 Stat. 374 (1980); see also, Earl W. Kintner et al., "The Effect of the Federal Trade Commission Act of 1980 on the FTC's Rulemaking and Enforcement Authority," *Washington University Law Review* 58:4 (1980), 847. https://goo.gl/ZZaxST.

17. Fair Credit Reporting Act, Pub. L. No. 90-321, 84 Stat. 1127 (1970).

18. Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (1996).

19. Children's Online Privacy Protection Act of 1998, Pub. L. No. 105-277, 112 Stat. 2681 (1998).

20. See, 15 U.S.C. § 45(a)(2).

21. See, Protecting and Promoting the Open Internet, *Report and Order on Remand, Declaratory Ruling, and Order*, GN Docket No. 14-28 (Mar. 12, 2015) ["2015 Open Internet Order"]. https://goo.gl/QafQCE.

The FCC has recently begun the process of reversing the 2015 Open Internet Order's Title II reclassification,[22] which would restore the FTC's jurisdiction over broadband, but the outcome of this proceeding is far from certain and it could likely be reversed by a future FCC. Thus, many scholars have recently called for Congress to eliminate or amend the common-carrier exemption to give the FTC clear authority over broadband, irrespective of how the FCC classifies it going forward.[23] Such an action would resolve the FTC-FCC jurisdictional turf war, but would leave substantial overlap between the purviews of the two agencies. As such, a clear division of responsibilities would still be required in order to avoid future conflicts.

Legal standards and tools

The FTC's legal standards for regulating commercial cybersecurity practices are the prohibitions in Section 5 of the FTC Act on "unfair methods of competition" and "unfair or deceptive acts or practices in or affecting commerce."[24] The former prohibition is the source of the FTC's antitrust authority, while the latter is the source of its consumer-protection authority.

While cybersecurity practices could theoretically constitute unfair methods of competition, it is more often the case that cybersecurity enforcement actions are brought under the FTC's unfairness and deception authority.[25] Using this authority, the FTC has brought more than 60 enforcement actions against private companies for maintaining inadequate cybersecurity practices.[26] Assuming the FTC can prove that the cybersecurity practices in question did violate Section 5 in such cases, the agency has multiple tools available to remedy the unlawful conduct, including "implementation of comprehensive privacy and security programs, biennial assessments by independent experts, monetary redress to consumers, disgorgement of ill-gotten gains, deletion of illegally obtained consumer information, and provision of robust transparency and choice mechanisms to consumers."[27]

In addition to case-by-case enforcement, the FTC also holds public workshops, issues reports, conducts surveys and offers other types of informal guidance to consumers and businesses about how to maintain good cybersecurity.[28] Unlike formal adjudications, such informal guidance is not binding on the agency, which makes it significantly less valuable to businesses trying to ensure that their cybersecurity practices comply with the law. However, in *FTC v. Wyndham Worldwide Corp.*, the Third U.S. Circuit of Appeals held that such informal guidance, on its own, can provide industry with enough guidance to comport with constitutional due process.[29]

Enforcement experience

Since 2002, the FTC has brought hundreds of enforcement actions in the areas of privacy and data security, with more than 60 on the latter issue alone.[30] This enforcement experience is substantial, and it includes key victories for consumers against such major tech companies as Uber,[31] Oracle,[32] Snapchat,[33] Twitter[34] and Microsoft.[35]

With only three exceptions, every cybersecurity enforcement action brought by the FTC has resulted in a consent decree. Under these decrees, the FTC can obtain certain remedies — such as remediation measures and compliance monitoring — that would be otherwise unavailable in an enforcement action. Such added flexibility can provide significant benefits for consumers, the agency and the parties to the enforcement action (who can avoid admitting liability in exchange for voluntarily agreeing to perform certain steps to remediate the problem). However, such consent decrees do not provide formal guidance to other industry actors on how to comply with the law going forward, in true common-law style.

Past FTC commissioners have touted the benefits of consent decrees, even going so far as to describe their enforcement style as the "common law of consent decrees," but the lack of formal guidance to industry creates substantial uncertainty.[36] More recently, the FTC has made a commendable effort to

22. See, Restoring Internet Freedom, *Notice of Proposed Rulemaking*, WC Docket No. 17-108 (May 23, 2017) ["Restoring Internet Freedom NPRM"]. https://goo.gl/jt3SJH.

23. See, e.g., Alden Abbot, "Time to Repeal the FTC's Common Carrier Jurisdictional Exemption (Among Other Things)?", The Heritage Foundation, Oct. 18, 2016. https://goo.gl/8KYUEM.

24. 15 U.S.C. § 45(a).

25. See, U.S. Federal Trade Commission, "Privacy & Data Security Update: FTC 2016 Privacy and Security Report" January 2017. https://goo.gl/8CaUgE.

26. Ibid.

27. Ibid.

28. Ibid.

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

30. FTC 2016 Privacy and Security Report, *supra* note 23.

31. U.S. Federal Trade Commission, *In re Uber Technologies, Inc.* (Aug. 21, 2017). https://goo.gl/U6dS2H.

32. U.S. Federal Trade Commission, *In re Oracle Corp.* (March 29, 2016). https://goo.gl/x1f1n7.

33. U.S. Federal Trade Commission, *In re Snapchat, Inc.* (Dec. 31, 2014), https://goo.gl/CCXuTG.

34. U.S. Federal Trade Commission, *In re Twitter, Inc.* (March 11, 2011). https://goo.gl/W4hAVf.

35. U.S. Federal Trade Commission, *In re Microsoft Corp.* (Dec. 24, 2002). https://goo.gl/mzRVut.

36. See, e.g., Berin M. Szóka, "Indictments Do Not a Common Law Make: A Critical Look at the FTC's Consumer Protection 'Case Law'," TPRC 2014, July 26, 2015. https://goo.gl/sCV3k5.

establish more formal guidance in the area of cybersecurity, both by litigating more cases in court[37] and by issuing more closing letters when an investigation determines that no violation has occurred.[38] These positive steps suggest that the FTC has recognized the importance of formal guidance in the area of cybersecurity. One hopes the agency will continue working to establish formal guidance going forward as cybersecurity practices and threats continue to evolve.

CYBERSECURITY REGULATION AT THE FCC

In contrast to the FTC, the FCC is a sector-specific agency charged with regulating the communications industry. Accordingly, its jurisdiction is more limited, as are its enforcement tools. However, the FCC has more experience regulating cybersecurity in certain areas, and it also has broad authority to supplement its flexible legal standards with more specific rules, as necessary.

For these reasons, it is sensible for the FCC to continue regulating cybersecurity practices in the areas where it is the relative expert, such as with emergency services. However, the lion's share of cybersecurity regulation should be done by the FTC, given its more comprehensive jurisdiction, enforcement tools and institutional experience. The question that remains is where the line between the two should be drawn.

Jurisdictional scope

The FCC administers the Communications Act of 1934, as it has been amended over the years to embrace new technologies and facilitate the transition from a nationwide monopoly telecommunications network to a competitive environment.[39] Provided in Title I of the Communications Act, the FCC's jurisdictional scope covers "all interstate and foreign communications by wire or radio."[40] The remainder of the Communications Act provides more specific regulatory authority for certain types of communications, including telecommunications services (Title II), broadcast services (Title III) and multichannel video programming services (Title VI).

Critically, the FCC has consistently distinguished between communications, on the one hand, and computer processing, on the other.[41] While the former has traditionally been heavily regulated as a common-carrier service under Title II of the Communications Act, the latter has traditionally been only lightly regulated under Title I of the Communications Act, unless the computer processing at issue is merely being used to operate a communications network.[42]

In the early 2000s, the FCC classified broadband service as an integrated "information service" under Title I of the Communications Act, which left the FTC free to regulate broadband service under its Section 5 authority. This decision was upheld in a 6-3 U.S. Supreme Court decision in 2005.[43] However, in early 2015, the FCC reversed course and reclassified broadband under Title II, finding that the computer processing inherent in broadband service fit within the exception for management of a telecommunications network.[44] This change in policy was upheld 2-1 in 2016 by the U.S. Court of Appeals for the D.C. Circuit,[45] although the possibility of Supreme Court review remains.[46] The commission is also currently considering whether to undo the 2015 order's Title II reclassification on its own.[47] At least for now, the FCC has broad authority to regulate broadband (under Title II), and the FTC has no regulatory authority over broadband, including the cybersecurity practices maintained by broadband providers.

Legal standards and tools

Under Title II of the Communications Act, the FCC has broad authority to regulate not only telecommunications services (which currently includes broadband), but also all "charges, practices, classifications, and regulations *for or in connection with*" broadband.[48] Thus, while the FTC has lost its authority to regulate broadband, the FCC has ample authority to step in and regulate such services, including the cybersecurity practices maintained by broadband providers, to ensure that they are "just and reasonable."[49]

In terms of legal standards, the FCC's "just and reasonable" standard is similar to the FTC's "unfair or deceptive" one, in

37. See, e.g., *FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015); LabMD, Inc. v. FTC, 776 F.3d 1275 (11th Cir. 2015); and U.S. Federal Trade Commission, *In re D-Link* (May 22, 2017). https://goo.gl/VCxcEm.

38. See, Allison Grande, "FTC Bureau Head Wants More Privacy Closing Letters Issued," *Law 360,* Dec. 3, 2014. https://goo.gl/mxhES5.

39. See, e.g., U.S. Federal Communications Commission, "About the FCC," Nov. 5, 2015. https://goo.gl/iSEvGQ.

40. 47 U.S.C. § 152(a).

41. See, e.g., *Nat'l Cable & Telecomms. Assoc. v. Brand X Internet Servs.*, 545 U.S. 967, 975–77 (2005).

42. See, ibid.; 47 U.S.C. 153(24) defines "information service" as "the offering of a capability for generating, acquiring, storing, transforming, processing, retrieving, utilizing, or making available information via telecommunications, and includes electronic publishing, *but does not include any use of any such capability for the management, control, or operation of a telecommunications system or the management of a telecommunications service*." (emphasis added).

43. *Nat'l Cable & Telecomms. Assoc. v. Brand X Internet Servs.*, 545 U.S. at 974 (2005).

44. See, 2015 Open Internet Order, *supra note* 19, ¶ 356.

45. *U.S. Telecomm. Ass'n v. FCC*, 825 F.3d 674 (D.C. Cir. 2016).

46. See, e.g., Jonathan Spalter, "Seeking a Supreme Court Review of Open Internet Rules," US Telecom, Sept. 28, 2017. https://goo.gl/d1gQbT.

47. See, Restoring Internet Freedom NPRM, *supra* note 20, ¶ 23.

48. 47 U.S.C. § 202(b). (emphasis added).

49. Ibid.; 47 U.S.C. § 222 provides a general duty that telecommunications carriers have to ensure that the proprietary information of their subscribers is adequately protected.

that a practice that is unfair or deceptive would also surely be unjust or unreasonable. Indeed, the terms "just" and "reasonable" are synonyms, so the FTC's unfairness and deception standards are basically more specific iterations of the FCC's.

However, while the FTC's rulemaking authority is strictly limited, the FCC has broad rulemaking authority that it can use to supplement its flexible legal standards with more specific requirements.[50] So, for example, if the FCC decided that all broadband providers should be required to implement a certain feature into their cybersecurity practices — such as two-factor authentication or biometric identification — the agency could accomplish such a goal via adjudication or rulemaking.[51] The added benefit of broad rulemaking authority may be useful in the context of cybersecurity. However, because such rules are more permanent — and, thus, less flexible — than adjudicatory precedent, they can also be harmful if they become outdated and ineffective or counterproductive as a result.

In terms of enforcement tools, the FCC's options are more limited than the FTC's. Like the FTC, the FCC can issue consent decrees with various behavioral requirements, but only if the party agrees to settle the FCC's investigation.[52] If the party at issue refuses to settle, the only remedy available to the FCC is a fine, the proceeds of which go to the U.S. Treasury Department.[53] Unlike the FTC, the FCC has no authority to order consumer redress, including disgorgement of ill-gotten gains and refunds.[54] The FCC also has a statute of limitations of one year,[55] while the FTC's statute of limitations in civil enforcements is five years.[56]

Enforcement experience

While the FCC has substantial experience regulating the cybersecurity of certain services, including mobile telephony[57] and emergency services,[58] its experience regulating cybersecurity more broadly is quite limited. Indeed, the body within the FCC tasked with such regulation, the Cybersecurity and Communications Reliability Division, is housed within the FCC's Public Safety and Homeland Security Bureau, which indicates the limited scope of its activities.[59]

Outside the context of calling records, E911 and emergency alerts, the FCC has brought only a single enforcement action regarding cybersecurity, which resulted in a consent decree and thus established no binding legal precedent.[60] The FCC has also published some informal guidance on cybersecurity practices on its website,[61] but the usefulness of such guidance to industry seems very limited, even as far as informal guidance goes.

Of course, in the context of emergency services, the FCC has substantial experience bringing enforcement actions for inadequate cybersecurity practices.[62] Without a doubt, it is the agency with the most experience in that area. For this reason, it should continue to regulate emergency services going forward, including the cybersecurity practices maintained by providers of such services. However, outside this discrete area, the FTC arguably is better suited to regulate commercial cybersecurity practices.

JURISDICTIONAL OVERLAPS AND REGULATORY CONFLICTS

As previously mentioned, the FCC's 2015 Open Internet Order sparked a jurisdictional turf war between the FCC and FTC, which was focused on the common-carrier exemption in the FTC Act. While much of the battle hinges upon the FCC's regulatory classification of broadband, the fight over Title I versus Title II is not the only relevant consideration here. Another important source of conflict is the interpretation of the exemption itself.

Both FTC and FCC officials have long maintained that the common-carrier exemption is activities-based, rather than

50. See. e.g., U.S. Federal Communications Commission, "Rulemaking Process," Nov. 3, 2015. https://goo.gl/usTxKo

51. See, e.g., SEC v. Chenery Corp., 332 U.S. 194, 203 (1947) ("[T]he choice made between proceeding by general rule or by individual, ad hoc litigation is one that lies primarily in the informed discretion of the administrative agency.") (citing *Columbia Broadcasting System v. United States*, 316 U.S. 407, 421 (1942)).

52. See, e.g., Joshua D. Wright, *Wrecking the Internet to Save it? The FCC's Net Neutrality Rule*, Testimony Before the U.S. House of Representatives, Committee on the Judiciary (March 25, 2015), p. 17. https://goo.gl/bs6dJH.

53. Ibid.

54. Ibid.

55. Ibid.

56. U.S. Federal Trade Commission, *Policy Statement Regarding Duration of Competition and Consumer Protection Orders*, 60 Fed. Reg. 42569, 42572 n.8 (Aug. 16, 1995). https://goo.gl/jiaEpG.

57. U.S. Federal Communications Commission, "Customer Privacy," 2017. https://goo.gl/M5LTiZ.

58. U.S. Federal Communications Commission, "Emergency Communications," Sept. 8, 2017. https://goo.gl/QVYMZS.

59. U.S. Federal Communications Commission, "Cybersecurity and Communications Reliability Division, Public Safety and Homeland Security Bureau," July 24, 2017. https://goo.gl/uxg7QB.

60. See, e.g., In re TerraCom, Inc. & YourTel America, Inc., *Order*, EB-TCD-13-00009175 (July 9, 2015). https://goo.gl/gZb52N; and Samuel Goldstick, "FCC Settles First Data Security Enforcement Action," Technology Law Dispatch, Aug. 25, 2015. https://goo.gl/C9BaA3.

61. U.S. Federal Communications Commission, "Cyber Security and Network Reliability," 2017. https://goo.gl/U8di8z.

62. See, e.g., Knutson, *supra* note 2.

status-based.[63] Under the FTC's interpretation, if a corporation offers some common-carrier services (e.g., telephony) and some other services (e.g., home security monitoring), then the common-carrier services are outside its jurisdiction, but it is still free to regulate all the other services. However, in a recent case against AT&T, a panel of judges in the Ninth U.S. Circuit Court of Appeals found that the common-carrier exemption is actually status-based.[64] Under that interpretation, if a corporation offers any common-carrier services, then the corporation is a common carrier and the FTC has no authority over its business practices.

This interpretation is perhaps reasonable in the context of AT&T, which mainly offers various forms of communications services, but the interpretation could lead to truly absurd results in other contexts. For example, if AT&T completes its pending acquisition of Time Warner, the status-based interpretation would mean that Time Warner (the content conglomerate behind HBO, not to be confused with the cable company that recently merged with Charter Communications and Bright House Networks) is immune from FTC oversight. Even worse, the status-based interpretation would put a company like Alphabet, which provides some common-carrier services through its Google Fiber and Project Fi subsidiaries, completely outside the FTC's jurisdiction, and would leave the FCC as the only agency with authority to regulate other Alphabet subsidiaries, like Google and YouTube, both of which offer no communications services. It would also potentially allow a corporation to evade all FTC jurisdiction simply by acquiring a *de minimis*[65] amount of common-carrier services (e.g., a small telephone company in rural Alaska), which potentially creates even more havoc in the legal system.

Thankfully, the full Ninth Circuit has agreed to rehear the AT&T case *en banc*,[66] and has indicated that the panel's decision should not be cited as legal precedent.[67] This suggests the status-based interpretation may soon be overturned in favor of the activities-based interpretation, but at least for now, the conflict between the FTC's and FCC's jurisdictions is intractable (at least, in the Ninth Circuit's jurisdiction). If the panel's decision is not overturned by the full Ninth Circuit or by the Supreme Court, Congress must step in as soon as possible to settle the issue and clarify that the FTC Act's exemption is only over common-carrier *services*, and not common carriers, writ large.

POTENTIAL DIVISIONS OF RESPONSIBILITY

In dividing responsibilities for commercial cybersecurity regulation between the FTC and FCC, there are multiple options available. One would be for the FCC to regulate the cybersecurity of data "in transit" while the FTC regulates the cybersecurity of data "at rest." A second option would be for the FCC to regulate the cybersecurity of all common carriers, while the FTC regulates the cybersecurity of all other commercial entities. A third option would be for the FCC to regulate the cybersecurity of common-carrier services, while the FTC regulates the cybersecurity of all other commercial services.

Each of these potential options has benefits and drawbacks, which will be discussed in turn. While each option has some appeal, on balance, the optimal division of cybersecurity responsibilities seems to be the third one, wherein the FCC is in charge of regulating the cybersecurity practices of common-carrier services, including emergency services, while the FTC regulates all others.

Data in transit

One option for dividing responsibilities for commercial cybersecurity regulation would be to focus on the nature of the data that needs protection. A common distinction made in the study of cybersecurity is between data "at rest" and data "in transit."[68] Cybersecurity is important for data in both of these states, since hackers can compromise data while it is "at rest" on a computer — a typical breach scenario — or while it is "in transit" over a communications network — a typical man-in-the-middle scenario.[69]

The main appeal of dividing responsibility for commercial cybersecurity regulation along these lines is that it largely mirrors the traditional distinction the FCC has made between communications and computer processing. Theoretically, given the FCC's experience ensuring network reliability and the integrity of communications — including telephony and other services, like emergency alerts — it could be best able to safeguard against man-in-the-middle attacks that take place mid-communication (i.e., while data are in transit from one place to another). This would leave the FTC to focus on the cybersecurity of data at rest.

63. See, e.g., John Eggerton, "FCC to Court: FTC Common Carrier Exemption is Activity Based," Broadcasting & Cable, June 2, 2017. https://goo.gl/QgwPNJ.

64. *FTC v. AT&T Mobility, LLC*, 835 F.3d 993 (9th Cir. 2016).

65. In legalese, the Latin phrase "de minimis" refers to something too trivial to merit consideration.

66. The term "en banc" refers to a full bench of judges, as compared to a mere panel, which is usually only three judges.

67. See, e.g., John Eggerton, "Ninth Circuit to Review FTC v. AT&T Mobility," Broadcasting & Cable, May 9, 2017. https://goo.gl/Wjtevx.

68. See, e.g., Nate Lord, "Data Protection: Data in Transit vs. Data at Rest," *Data Insider*, July 27, 2017. https://goo.gl/WCXYxB.

69. Ibid., ("Unprotected data, whether in transit or at rest, leaves enterprises vulnerable to attack, but there are effective security measures that offer robust data protection across endpoints and networks to protect data in both states.")

While conceptually appealing, there are significant drawbacks to this division of responsibilities. For example, some cybersecurity researchers make a further distinction between data states, including data "in use" as a third category. The lines between "at rest," "in use" and "in transit" may be very difficult to draw in practice and could lead to the very regulatory conflicts the division of responsibilities seeks to avoid.[70] Moreover, there is substantial overlap between the security practices used to protect data at rest and data in transit (e.g., encryption), so having two different agencies oversee the implementation of the same cybersecurity practices would be inefficient, at best, and counterproductive, at worst, if the guidance issued by the FTC conflicts with that issued by the FCC.

Thus, while dividing responsibilities along the lines of what state the data at issue are in has some conceptual appeal, this division would likely not work very well in practice.

Common carriers

A second option for the division of responsibilities would be to focus on the type of business being regulated. As discussed above, the FTC has no jurisdiction over common carriers — at least, insofar as they offer common-carrier services, if not across the board. So, theoretically, the FCC could be responsible for regulating the cybersecurity of all common carriers while the FTC is responsible for regulating all other business entities.

This structure is currently the law of the land within the Ninth Circuit's jurisdiction. However, as discussed above, it could potentially lead to some absurd outcomes, where the FCC is tasked with the responsibility of regulating services that in no way resemble the communications services with which it has experience. Of course, some might prefer that the FCC use its broader common-carrier and rulemaking authority to regulate major tech companies, like Facebook and Google.[71] However, for various reasons, this approach would be a huge mistake.[72]

Arguably, it may be simpler for regulatory authority over a company to be assigned to a single agency, rather than having multiple agencies regulate separate services offered by a single company, based on the nature of those services. However, that simplicity would come at significant cost, as it may require the FCC to regulate services that are outside its area of expertise and with tools that are unfit for the purpose.

While the Ninth Circuit effectively endorsed this division of responsibilities, the decision will hopefully be overturned in the near future. The assignment of regulatory authority over an entire company simply because it offers some type of common-carrier service is unwise, and thus this option is not a viable one.

Common-carrier services

A third possibility for dividing responsibility for commercial cybersecurity regulation would be to focus on the nature of the services being regulated. Specifically, the FCC could be responsible for regulating the cybersecurity of all common-carrier services, while the FTC regulates the cybersecurity practices of all other services. This is the division of responsibilities that the FTC and FCC both endorsed, with respect to the common-carrier exemption being activities-based rather than status-based. For this reason, restoring such a division should help resolve the ongoing jurisdictional turf war between the two agencies. This option would also allow the FCC to focus on what it knows best (i.e., how to maintain the reliability of communications networks) without tasking it with regulating areas outside its experience and expertise.

However, even if the distinction between common-carrier and other services is clearly the most sensible division, the question remains as to whether the FCC's common-carrier authority covers broadband or merely telephony. The FCC clearly has the most experience and expertise regulating the latter, and for this reason, it should continue to do so, along with other services that utilize the Public Switched Telephone Network and North American Numbering Plan. Crucially, this would cover E911 and emergency alert systems, which have long been overseen by the FCC's Public Safety and Homeland Security Bureau. Whether the cybersecurity of broadband should be regulated by the FCC, FTC or both, is a more difficult question.

Comparatively, the FTC has more experience regulating broadband cybersecurity than the FCC, which has had chief responsibility in the area for only a couple of years. Moreover, given the overlap between the cybersecurity practices relevant to broadband service and those relevant to other services (encryption, firewalls, etc.), it is likely that the FTC's broader cybersecurity experience could be very useful in the context of broadband. Thus, the FTC should have authority over broadband cybersecurity.

For that to happen, either the FCC must undo the 2015 Open Internet Order's Title II reclassification, or Congress must repeal or amend the common-carrier exemption in the FTC Act to give the FTC clear authority over broadband. Both of these actions have merit, and it is unclear if one should necessarily be done to the exclusion of the other. It is, however, imperative that at least one be done, if not both. The result

70. See, e.g., Bob Janacek, "Best Practices: Securing Data at Rest, in Use, and in Motion," Data Motion, Dec. 1, 2015. https://goo.gl/oujBPG.

71. See, e.g., Andrew Orlowski, "Steve Bannon Wants Facebook, Google 'Regulated like Utilities,'" *The Register,* July 31, 2017. https://goo.gl/6qwkug.

72. See, e.g., Tom Struble, "For Internet Gatekeepers, Consumer Protection Laws are Better than Utility-Style Regulation," *TechTank*, Sept. 26, 2017. https://goo.gl/HbJTMq.

may be a jurisdictional overlap between the FTC and FCC, but regulatory conflicts can still be avoided in such a case through effective communication between the two agencies when it comes to guidance and enforcement.[73] This is the most logical division of responsibilities for commercial cybersecurity regulation between the FTC and FCC, and it should yield the optimal regulatory outcomes in practice.

CONCLUSION

Given the vast importance of cybersecurity in the modern world, it is vitally important that sensible market-based and regulatory mechanisms are available to discipline cybersecurity practices. There are multiple options for how responsibilities for commercial cybersecurity regulation could be divided between the FTC and FCC. However, the most logical division of responsibilities is for the FCC to regulate the cybersecurity of all "common-carrier services," — including telephony and emergency services — while the FTC regulates the cybersecurity practices of all other services, including broadband. Depending on the future of broadband regulation at the FCC, both agencies may have a role to play in regulating broadband cybersecurity. But if such jurisdiction is to be given to both agencies, regulatory conflicts between the two must be avoided through proper cooperation and coordination.

ABOUT THE AUTHOR

Tom Struble is technology policy manager and a policy analyst with the R Street Institute, where he leads R Street's work on telecom, antitrust, privacy and data-security issues. His role also calls for him to meet with policymakers and stakeholders, file regulatory comments and amicus briefs, and write op-eds, coalition letters and white papers.

Tom joined R Street in May 2017 from TechFreedom, where he worked as policy counsel focused mostly on telecom and consumer-protection issues, with an eye toward antitrust and market-oriented policy solutions. He previously worked as a law clerk for the Competitive Carriers Association and for the mobility division of the Federal Communications Commission's Wireless Telecommunications Bureau. Earlier in his career, he interned with the office of then-U.S. Rep. Jerry Moran, R-Kan.

73. See, e.g., U.S. Federal Trade Commission, "FTC and FCC Sign Memorandum of Understanding for Continued Cooperation on Consumer Protection Issues," Press Release, Nov. 16, 2015. https://goo.gl/mZS29q.