1212 New York Ave., N.W.
Suite 900
Washington, DC 20005
202.525.5717


***Free Markets. Real Solutions.***
***www.rstreet.org***

| | | |
|---|---|---|
| In the Matter of | ) | |
| Developing the Administration's Approach to Consumer Privacy | ) | Docket No. 180821780-8780-01 |

# Comments of R Street Institute

Respectfully submitted,

**/s/**

Charles Duan
*Tech Policy Director*

Joe Kane
*Tech Policy Fellow*

Tom Struble
*Tech Policy Manager*

Caleb Watney
*Tech Policy Fellow*

Jeff Westling
*Tech Policy Associate*

November 9, 2018

# Table of Contents

## I. Introduction

In this proceeding, the National Telecommunications and Information Administration ("NTIA"), on behalf of the Department of Commerce, is seeking public comments on various issues relating to consumer privacy.[1] Given the changing nature of the economy and recent legal developments both abroad and among the various states, a comprehensive review of the Administration's approach to consumer privacy is both appropriate and timely.

To aid in the development of the Administration's approach to consumer privacy, the R Street Institute ("R Street" or "RSI") hereby submits the following comments, which comprise summaries and attachments of our past work on various consumer-privacy issues. These studies and commentaries should help guide the Administration in determining the best path toward protecting consumer privacy while fostering innovation and competition.

## II. Summary of RSI Work on Various Consumer-Privacy Issues

R Street's mission is to engage in policy research and outreach to promote free markets and limited, effective government. That mission includes policy research and outreach on issues relating to consumer privacy and data protection. The work generated through this research and outreach is briefly summarized below and attached hereto as Appendices A through P.

[1] Developing the Administration's Approach to Consumer Privacy, *Notice; Request for Public Comments*, GN Docket No. 180821780-8780-01 (Sept. 26, 2018) [hereinafter RFC], https://goo.gl/o67JrN.

**A. Tom Struble & Joe Kane, "New Internet Privacy Bill Would Bring European-Style Regulations," *The Daily Caller* (May 31, 2017)**

This opinion piece analyzes the BROWSER Act, a bill introduced by Representative Blackburn (R-Tenn) in early 2017, and critiqued aspects of the legislation that were overly broad or prescriptive.

**B. Tom Struble & Joe Kane, "A Three-Step Plan to Promote Consumer Privacy," *Morning Consult* (June 26, 2017)**

This opinion piece offers three concrete steps that Congress can take to improve consumer privacy: (1) repeal the Federal Trade Commission ("FTC") Act's common-carrier exemption; (2) preempt the patchwork of state privacy laws and establish a uniform national framework; and (3) provide the FTC with the direction and resources necessary to update and enforce that national privacy framework.

**C. Tom Struble, "For Internet Gatekeepers, Consumer Protection Laws are Better than Utility-Style Regulation," *Brookings TechTank* (Sept. 26, 2017)**

This opinion piece touches on net neutrality and other issues relating to potential discrimination by so-called "Internet gatekeepers," arguing that flexible, ex post adjudication using consumer-protection laws is preferable to inflexible, ex ante utility-style regulation for dynamic industries like telecommunications and e-commerce.

**D. Tom Struble, "Senate Finally Poised to Restore FTC to Full Strength," *R Street Blog* (Oct. 19, 2017)**

This opinion piece applauds the Administration for selecting qualified candidates to fill the open Commissioner spots at the FTC, which is especially vital at this time when key consumer-protection issues, including privacy, are in flux.

**E. Tom Struble, "Resolving Cybersecurity Jurisdiction Between the FTC and FCC," *R Street Policy Study No. 116* (Oct. 2017)**

This policy study examines the respective roles of the FTC and the Federal Communications Commission ("FCC") in regulating cybersecurity issues—as well as several recent court cases and regulatory actions that have thrown those roles into question—before assessing three proposals for how to best divide cybersecurity responsibilities between the two agencies.

**F. Tom Struble, "Reforming the Federal Trade Commission Through Better Process," *R Street Policy Study No. 122* (Dec. 2017)**

This policy study identifies key weaknesses in agency process at the FTC, analyzes the negative effects that stem from those weaknesses, and offers several proposals for how to strengthen agency process to ultimately improve regulatory outcomes in areas like consumer privacy.

**G. Tom Struble, "A Positive Agenda for the New FTC," *Morning Consult* (Feb. 14, 2018)**

This opinion piece offers a positive agenda for the new FTC to pursue, which includes three key pillars: (1) litigating more privacy and data security cases in order to establish more formal precedent to guide industry practices; (2) putting up or shutting up on net neutrality so that Congress can decide whether to leave it with the FTC or move it back to the FCC; and (3) looking beyond the swamp to tackle occupational licensing and other regulatory barriers to competition at the state and local levels.

**H. Charles Duan et al., "Policy Approaches to the Encryption Debate," *R Street Policy Study No. 133* (Mar. 2018)**

This policy study examines encryption technology, which is a key way for individuals to protect their personal privacy but has long been the subject of debate due to its effects on law enforcement. As part of that examination, R Street proposes a framework for

evaluating the encryption debate in a manner that balances law-enforcement concerns with consumer-privacy interests.

**I. Charles Duan, "A New Framework for the Encryption Debate," *Lawfare* (Apr. 9, 2018)**

This opinion piece draws on the encryption policy study summarized above to describe the proposed new framework for the encryption debate in a format that is shorter and more easily digestible for readers.

**J. Tom Struble, "New FTC Leadership Should Focus on Results, Not Headlines," *Morning Consult* (May 18, 2018)**

This opinion piece encourages the new FTC leadership to focus on achieving real results—in terms of both remedies for consumers and doctrinal victories in court—rather than pursuing high-profile actions that generate lots of headlines but ultimately have little impact on the market.

**K. Caleb Watney, "Comments of the R Street Institute on the Consumer Welfare Implications Associated with the Use of Algorithmic Decision Tools, Artificial Intelligence and Predictive Analytics," Docket No. FTC-2018-0056 (Aug. 13, 2018)**

These comments emphasize the importance of examining international regulatory competition and the way that innovation flows across borders. It argues that we cannot simply create our ideal privacy framework in a vacuum and instead must consider the way that tightening privacy laws could make artificial-intelligence ("AI") development relatively more advantageous in countries like China.

**L. Tom Struble, "Comments of the R Street Institute on the State of Antitrust and Consumer Protection Law and Enforcement, and Their Development, Since the Pitofsky Hearings," Docket No. FTC-2018-0048 (Aug. 14, 2018)**

These comments assess the current state of antitrust and consumer-protection law and how things have changed in these areas since the FTC's Pitofsky hearings in the 1990s,

arguing that recent changes in technology require a recommitment to economic analysis and consumer welfare but not a fundamental reformation of these areas of law.

**M. Tom Struble, "Comments of the R Street Institute on the Commission's Remedial Authority to Deter Unfair and Deceptive Conduct in Privacy and Data Security Matters," Docket No. FTC-2018-0052 (Aug. 14, 2018)**

These comments assess the FTC's recent use of its consumer-protection authority to detect and punish unfair or deceptive conduct in privacy or data security, urging the FTC to learn from its recent *Wyndham* and *LabMD* cases and to also continue exploring the difficult issue of informational injuries.

**N. Tom Struble, "European Competition Law is Hurting Consumers," *National Review* (Sept. 6, 2018)**

This opinion piece analyzes the European Commission's recent enforcement against Google for how it licenses the Android mobile operating system to equipment manufacturers, arguing that the Commission's analysis was flawed in key respects and will ultimately harm consumers by elevating the interests of competitors over theirs.

**O. Caleb Watney, "Reducing Entry Barriers in the Development and Application of AI," *R Street Policy Study No. 153* (Oct. 2018)**

This policy study argues that there are a host of policy barriers making it difficult for startups to compete with incumbent firms in AI development and application. One of the areas highlighted in the study was the potential for excessive privacy laws to disincentivize data sharing, which would disproportionally hurt startups and small businesses.

**P. Jeffrey Westling, "Can BuzzFeed Save Us from Deep Fakes?" *Morning Consult* (Oct. 23, 2018)**

This opinion piece examines issues presented by AI-generated fake video and argued that such technology presents no unique challenges compared to other tools for deceiving consumers, meaning that strict government oversight is unnecessary.

## III. Conclusion

The Administration should be commended for launching this proceeding and seeking public comment on ways to improve the current state of consumer privacy in the United States. We are pleased to contribute our work to this process and we look forward to engaging further with the Administration, federal regulators, and other stakeholders as it proceeds.

Respectfully submitted,

**/s/**

Charles Duan
*Tech Policy Director*

Joe Kane
*Tech Policy Fellow*

Tom Struble
*Tech Policy Manager*

Caleb Watney
*Tech Policy Fellow*

Jeff Westling
*Tech Policy Associate*

November 9, 2018

# NEW INTERNET PRIVACY BILL WOULD BRING EUROPEAN-STYLE REGULATIONS

6:02 PM 05/31/2017 | OPINION
**Tom Struble & Joe Kane | R Street Institute**

As debate over the future of internet regulation drags on, Representative Marsha Blackburn, R-Tenn., Chairwoman of the House Energy and Commerce Committee's Communications and Technology Subcommittee, introduced, amid strong public backlash against Congress's repeal of FCC privacy regulations, a surprising new bill (H.R. 2520) regarding the privacy of users' online information: the BROWSER Act. The bill would impose stronger privacy obligations on internet service providers (ISPs) and also require, for the first time that all websites, applications and other "edge companies"—firms like Google, Facebook and Amazon—obtain opt-in consent before tracking and using consumer data online.

This bill is surprising in many respects, not least of which is the fact that Blackburn was one of the chief forces pushing fellow Republicans to use the Congressional Review Act to repeal the FCC's broadband privacy rules from October 2016, notably requiring ISPs to get opt-in consent before collecting or sharing user data.

Opponents of the FCC rules noted that they created an unleveled playing field since edge providers would fall under the FTC's jurisdiction, requiring only that they offer a simple way for users to opt-out of such tracking, while ISPs were held to a more burdensome standard. The BROWSER Act would keep the playing field level, but subject ISPs and edge providers to the more burdensome opt-in standard, placing the FTC in charge of enforcing the rules for both groups.

This new regime would closely resemble the European privacy system, under which websites are mandated to display pop-up notifications whenever users visit a site and get opt-in consent before tracking or using their data (such as to sell ads or improve the site's services). This process provides additional privacy protections, but also renders online service less convenient for users and discourages data innovation. The comparatively flexible FTC privacy regime is a key reason why the U.S. has so many successful tech firms and such a vibrant online ecosystem, while Europe has failed to produce many firms of similar prowess.

It's commendable that Chairwoman Blackburn is trying to improve U.S. privacy laws, and Congress should move quickly to resolve the status of internet regulation and establish a layer-neutral approach to privacy. Harmonizing the regulatory regime for ISPs and edge providers also is a laudable goal. Similarly, the bill's preemption of patchwork and contradictory state laws that create regulatory uncertainty and compliance problems is also a positive step. Regulating everyone up to an opt-in standard, however, is a step in the wrong direction.

Conspicuously, the bill also makes no mention of the other side of the privacy coin: data security. Users are more willing to share their data when they have confidence it will be kept secure. The FTC has ample experience regulating data security, and any privacy bill should fix the current jurisdictional gap, preventing it from regulating ISPs.

It's important to note that consumer data shared with advertisers is not directly linked to any person—advertisers can't buy data about a particular individual. Rather the data are aggregated into broad demographic categories, which are then used to sell ads targeted toward those demographics. Collecting and sharing this kind of information is essential to the business model of many internet companies. Indeed, it is the reason why consumers can use so many great apps and websites without having to pay separate subscription fees for each.

While ads can be annoying, most people don't mind giving up some information in exchange for free services. Most people also prefer ads targeted to their interests over random ads. Furthermore, for those who want more privacy, numerous tools exist to serve that need that don't require changing the rules for the whole ecosystem. Privacy-oriented internet companies—like Ello and Duck Duck Go—have been around for years, but haven't attracted many users, which says a lot about people's privacy preferences (as revealed by their actions) and cautions against taking an overly precautionary approach that could have drastic consequences for internet commerce.

If the default is set against sharing information, expect less information to be shared and less innovative uses of data to be developed going forward. In a two-sided market, one in which ISPs and edge providers sell both their services to consumers and ad space to advertisers, diminishing the ability to collect from one side of the market (advertisers), will result in higher prices for the other side (consumers). Economists call this the "waterbed effect." So, while there are legitimate concerns about the extent to which user data should be shared, it's also important to recognize the real-world trade-off between strict default privacy rules and higher prices for online goods and services.

How to balance that trade-off is a choice consumers should make for themselves, rather than relying upon the benevolent paternalism of government. While both opt-out and opt-in regimes allow users to control their privacy and usage of their data, the default option should be the one that already reflects people's revealed preferences, and that keeps online services accessible to the greatest number of people. The current opt-out regime is thus the best mechanism to keep the internet free and innovative. In its current form, the BROWSER Act will do more harm than good.

*Tom Struble is tech policy manager and Joe Kane is tech policy associate or the R Street Institute*

TAGS : FEDERAL COMMUNICATIONS COMMISSION INTERNET INTERNET PRIVACY MARSHA BLACKBURN



https://dailycaller.com/2017/05/31/new-internet-privacy-bill-would-bring-european-style-regulations/

OPINION

# A Three-Step Plan to Promote Consumer Privacy

BY **TOM STRUBLE** & **JOE KANE**
June 26, 2017

Congress' decision to use the little-utilized Congressional Review Act to repeal broadband privacy regulations the Federal Communications Commission handed down in October has been met with less than universal approval. Bills to increase user control over online privacy have since been introduced by members of both parties, and in both chambers of Congress.

There is much to like in these bills, but each misses the mark in one way or another. Congress should be commended for trying to bolster Americans' privacy, but it's important to strike the appropriate balance. The wrong approach could fundamentally disrupt the internet ecosystem, which relies on advertising-supported business models to deliver countless benefits to consumers free of charge.

Nonetheless, there are steps Congress can and should take to improve consumer privacy. Here are three big ones.

First, Congress should repeal the common-carrier exemption. Historically, consumer-privacy regulation has been almost entirely the domain of the Federal Trade Commission. In the online space, all that changed when the FCC moved to reclassify broadband as a "common carrier" service in 2015. The FTC lost its jurisdiction, leaving broadband providers subject to different rules than the rest of the internet ecosystem.

This is untenable. It warps the playing field by giving some internet companies a leg up over others. Moreover, the lines between those two sets of companies are becoming increasingly blurred. We need a privacy regime that can protect consumers regardless what part of the internet ecosystem they're interacting with.

The FCC appears ready to undo the 2015 reclassification, but that will take months and may not hold up, either in court or through the next change in administration. Congress should step in now to close the jurisdictional gap between the two agencies by repealing the common-carrier exemption in the Federal Trade Commission Act and granting the FTC privacy authority across the board.

Second, Congress should pre-empt the current patchwork of state privacy laws by setting a single standard to govern consumer privacy throughout the country. Federalism is an important principle in American government, but internet services are inherently interstate commerce. The balance struck by the framers of the Constitution dictates that uniform federal rules should prevail in cases like this. Congress can better protect consumers and reduce compliance costs for industry by declaring the FTC's regime for regulating privacy and consumer protection online the ultimate law of the land.

Third, Congress should direct the FTC to update its current privacy regime and reconsider which types of data are sensitive. The recent privacy backlash focused mostly on metadata, like one's history of browsing the web or using various apps. The contents of communications and other personal information like birthdays and Social Security numbers long have been deemed sensitive because exposure of that information can cause real harm to consumers – either reputational

damage like public embarrassment or financial damage like identity theft.

Metadata historically weren't deemed sensitive. In the analog era, exposure of such data carried little risk of harm. However, many now feel such information shouldn't be shared without a user's affirmative opt-in consent. Internet companies and data brokers increasingly can cobble together and analyze metadata to learn very personal things about users, which means exposure of such data carries greater risk in the digital era. For a potent example, one need look only to the reputational harms suffered by visitors to the Ashley Madison website when they were publicly outed two years ago.

Several recent congressional bills would affirmatively declare such metadata to be sensitive, but legislating that particular outcome could be a mistake. Strong privacy protections are good, but defining sensitivity too broadly can do real harm, and defining it too narrowly can leave consumers unprotected. For example, a privacy bill passed 10 years ago might have covered web browsing but not applications, which are increasingly how consumers engage online.

The FTC, as the expert agency, should be in charge of deciding what types of data are sensitive and what forms of notice and choice are required for different types of data. Congress should simply tell the FTC to adjust its approach to better reflect the current privacy landscape. This could be done through a congressional policy statement or a limited grant of rulemaking authority governing access to consumer metadata. Either approach would be vastly superior to the bills that have been put forward thus far.

15 | R Street Institute

*Tom Struble is a technology policy manager with the R Street Institute. Joe Kane is a tech policy associate at the R Street Institute.*

Morning Consult welcomes op-ed submissions on policy, politics and business strategy in our coverage areas. Updated submission guidelines can be found here.

TECH

BROOKINGS

TechTank

# For internet gatekeepers, consumer protection laws are better than utility-style regulation

Tom Struble Tuesday, September 26, 2017

Back in 2014, former Brookings scholar Robert Litan presciently warned that regulating broadband providers like public utilities in order to protect Net Neutrality, "could one day boomerang on certain major tech companies, too." Three years later, that boomerang is now coming back with a vengeance. As progressive luminaries like Tim Wu and Susan Crawford continue fighting for utility-style regulations for broadband providers, prominent conservatives like Tucker Carlson and Steve Bannon have begun demanding similar utility-style regulations for other internet "gatekeepers," including major websites and online platforms like Google and Facebook.

The targets are different, but the arguments attempting to justify these regulations are surprisingly similar. In a nutshell: big corporations have too much control over the free flow of information online, so the government must regulate internet gatekeepers like public utilities in order to protect users from harmful censorship or other discriminatory behavior.

Even if you accept the premise of that argument — and reasonable minds disagree over just how much control is too much for one corporation to have — it's far from clear that utility-style regulation is the proper response. Indeed, in the dynamic markets for internet services, imposing true utility-style regulations would be a huge mistake.

Public utilities can take multiple forms, but the hallmark of each is a lack of competition. The markets for broadband, search, social media, operating systems and other internet services may be concentrated — to varying degrees — but they don't fit the public-utility model, because real competition is possible (even if it's not as fierce as we'd like it to be).

The utility model denies that possibility, and is essentially a self-fulfilling prophecy: By giving up on market forces and ceding dominance to a single firm, utility-style regulation makes future competition impossible.

Left unchecked, this vicious cycle — where regulation depresses competition, thus justifying more regulation that further depresses competition, and so on and so forth — could wreak havoc throughout the internet ecosystem. Do we really want internet services to be provided by Government-backed monopolists, rather than by private firms competing to serve consumers in the best way possible?

Fortunately, strong antitrust and consumer protection laws can save us from this downward spiral of utility-style regulation. Antitrust law has regulated competition throughout the American economy for over a century, with fairly positive results. When internet gatekeepers used their market power to suppress innovation (AT&T), suppress competition (Microsoft) or fix prices (Apple), antitrust law was there to keep them in check. Thus, it's no surprise that a range of scholars are now calling for antitrust law to be used against today's internet gatekeepers, including in the context of Net Neutrality.

However, other scholars believe that antitrust alone isn't up to the task, as it has several potential shortcomings that are relevant here. For example, how would antitrust resolve difficult questions of market definition and substitutability in the context of the internet? And how can antitrust properly account for non-economic factors, like the various cultural and societal benefits enabled by the free flow of information online? That body of law is simply incapable of recognizing and accounting for various intangibles, like conceptions of fairness and equality, which we consider to be valuable goals.

Thankfully, we also have consumer protection law to draw upon. The classic model of consumer protection is Section 5 of the Federal Trade Commission Act, which prohibits all "unfair or deceptive acts or practices" in commerce. In the context of internet services and gatekeepers, this model could be used to great effect. For example, if a gatekeeper holds itself out as a neutral platform or conduit, but secretly engages in censorship or unfair discrimination, that's arguably "deceptive" and illegal. Similarly, if a gatekeeper fails to disclose relevant information to users (say, its policies for either publishing or blocking offensive speech), that's arguably "unfair" and illegal.

These basic consumer protection tools could resolve much of the concerns over Net Neutrality, too. Indeed, the Federal Communication Commission's 2015 Open Internet Order provided several consumer protection tools, including a "reasonableness" standard similar to the FTC's authority under Section 5 and a transparency rule requiring broadband providers to make certain disclosures regarding their traffic management practices, which might not be "unfair" to withhold, but which would make the internet ecosystem more open and competitive if disclosed. The FCC is likely to soon reconsider key portions of that Order, mostly because the utility-style regulations in Title II of the Communications Act (which were not enforced by the 2015 Order, but which remain on the books) are arguably depressing broadband investment.

Hopefully the FCC won't throw the baby out with the bath water. Removing the bright-line prohibitions on certain practices may be defensible, but the agency must not abandon its basic consumer protection framework for Net Neutrality. Ideally, that framework would closely mirror the FTC's approach under Section 5, so the standards for antitrust and consumer protection can apply consistently throughout the internet ecosystem. Some may feel that utility-style regulations are appropriate for some gatekeepers and not others, but this ignores the reality of the situation: broadband providers have the ability to block or censor information online, but so do websites, operating systems, registrars and many others.

In order to protect both consumers and competition, we need to regulate all of these internet gatekeepers, including broadband providers and other actors in the ecosystem with the power to censor or distort the free flow of information online. However, we shouldn't regulate them like public utilities, as that will only serve to depress competition and hurt consumers over the long run. We need to embrace strong antitrust and consumer protection laws instead.

---

*Google, Facebook, Microsoft, and AT&T are donors to the Brookings Institution. The findings, interpretations, and conclusions posted in this piece are solely those of the author and not influenced by any donation.*

Free markets. Real solutions.

OCT 19, 2017

**Senate finally poised to restore FTC to full strength**

Earlier today, President Donald Trump formally announced the three candidates he's nominating for the open seats at the Federal Trade Commission. Joseph Simons, Rohit Chopra, and Noah Phillips have diverse backgrounds and divergent political views, but they all have impeccable legal credentials and should be confirmed by the U.S. Senate without hesitation.

Not only will their confirmation put three more sets of steady hands at the wheel of the nation's chief consumer protection and antitrust agency, but it also will finally restore the FTC to full strength, freeing it up to once again take on the kinds of hard cases that tend to split public opinion.

The FTC, which has jurisdiction over nearly every sector of the U.S. economy (with only a few limited exceptions), has had only two commissioners for most of 2017, ever since outgoing Chairwoman Edith Ramirez resigned in early February. To their credit, Acting Chairwoman Maureen Ohlhausen and Commissioner Terrell McSweeny have done an admirable job finding common ground and working together where possible, including by blocking an allegedly anticompetitive merger in daily fantasy sports, imposing structural-separation requirements on a key merger in the semiconductor industry, settling a privacy suit against a major ridesharing service and, most recently, launching an investigation into the Equifax breach.

However, with a partisan deadlock in place, the commission has only been able to act when it had unanimous consent. This has left it unable to tackle difficult questions that truly push the bounds of precedent and drive the evolution of legal doctrine forward. By all accounts, Simons, Chopra and Phillips are all FTC scholars who should be ready to hit the ground running on day one. Each of them also has relevant personal experience that should hold them in good stead at the commission.

Joseph Simons, long-rumored to be Trump's pick for FTC chairman, comes most recently from the antitrust group at law firm Paul Weiss. He also spent time as director of the FTC's Competition Bureau in the early 2000s, working deeply on both mergers and other enforcement actions. Given the uptick in merger activity this year, Simons' experience in this area will surely come in handy at the FTC, which has a key role to play, along with the U.S. Justice Department, in reviewing proposed mergers and acquisitions to prevent potential harms to competition or consumers.

Rohit Chopra, the pick to fill the open Democratic slot, also has significant prior experience in the federal government. He served as assistant director of the Consumer Financial Protection Bureau and in 2011 was named by former Treasury Secretary Timothy Geithner to be the U.S. Treasury Department's first student loan ombudsman. Chopra is considered a darling of key Democrats like Senate Minority Leader Chuck Schumer, D-N.Y., and Sen. Elizabeth Warren, D-Mass., for his efforts to combat student loan debt and other financial burdens affecting young people. While his stance on for-profit colleges may rankle some Senate Republicans, there is no reason to think he won't be confirmed. After all, disagreements over policy aren't a valid reason

to deny confirmation of a qualified nominee (although members of both parties tend to forget that from time to time).

Finally, Noah Phillips was nominated to fill the final Republican vacancy at the FTC, and he also brings a decorated and interesting background to the table. Phillips previously spent time in civil litigation for both Steptoe & Johnson and Cravath, Swaine & Moore, but most recently has been serving as chief counsel for Senate Majority Whip John Cornyn, R-Texas, with the Senate Judiciary Committee. From his post on the Judiciary Committee, Phillips has oversight of the U.S. legal system as well as intellectual property, which should come in handy as the FTC continues to engage in more patent work, such as its review of patent assertion entities and its ongoing case alleging anticompetitive abuse of patents underlying equipment used in smartphones.

With a full complement of qualified commissioners, the FTC can once again function as an agency with the skills and capacity to tackle the key competition and consumer-protection issues. The Senate shouldn't delay to confirm all three nominees.

---

https://www.rstreet.org/2017/10/19/senate-finally-poised-to-restore-ftc-to-full-strength/#

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.

Free markets. Real solutions.

R STREET POLICY STUDY NO. 122
December 2017

# REFORMING THE FEDERAL TRADE COMMISSION THROUGH BETTER PROCESS

Tom Struble

CONTENTS



## INTRODUCTION

The Federal Trade Commission ("FTC" or "Commission") has been the chief consumer protection and competition agency in the United States for over 100 years.[1] During that time, this "uniquely compelling experiment in economic regulation"[2] has had mixed results. While the agency and the consumers it represents have enjoyed some tremendous victories along the way, there have also been some notable failures and missteps, which have resulted in numerous course corrections from the courts and Congress.

Such moments of conflict and transformation often followed periods of disruptive technological innovation, when business models, consumer habits and American lifestyles were undergoing tremendous change.[3] Arguably, we are in a similar period today, as advances in digital services, broadband connectivity and smartphone adoption continue to create new markets and disrupt existing ones—all of which dramatically changes the ways consumers behave and companies do business. In recent years, such changes have generated numerous conflicts and there are serious concerns that the FTC has not been handling them appropriately.[4] Moreover, in the near future, the FTC will once again be tasked with regulating the practices of broadband providers and policing any violations of Net Neutrality that threaten to harm consumers or competition.[5] Advances in artificial intelligence, automation and blockchain technologies will also surely present additional challenges for the FTC going forward.

Accordingly, it is imperative that the agency's processes are in good working order. While its missteps could be corrected by the courts, their limited scope of review may allow deficiencies to persist for longer than they should.[6] For this reason, a more direct path to reform is for Congress to amend the FTC Act and implement changes to the agency's processes directly. To this end, numerous reform bills have recently been proposed.[7] However, a full review of these is beyond the

1. See, e.g., Marc Winerman, "The Origins of the FTC: Concentration, Cooperation, Control, and Competition," *Antitrust Law Journal* 71:1 (2003), 1-97. https://goo.gl/GRZ6fh.

2. William E. Kovacic and Marc Winerman, "The Federal Trade Commission as an Independent Agency: Autonomy, Legitimacy, and Effectiveness," *Iowa Law Review* 100:5 (May 2015). https://goo.gl/VaXWtR.

3. See, e.g., J. Howard Beales, "The FTC's Use of Unfairness Authority: Its Rise, Fall, and Resurrection," Federal Trade Commission: The Marketing and Public Policy Conference, May 30, 2003. https://goo.gl/TZX9sJ.

4. See, e.g., Joshua D. Wright, "The FTC and Privacy Regulation: The Missing Role of Economics," George Mason University Law and Economics Center: Briefing on Nomi, Spokeo, and Privacy Harms, Nov. 12, 2005. https://goo.gl/AzMKH8.

5. See, e.g., In re Restoring Internet Freedom, Declaratory Ruling, *Report and Order, and Order*, WC Docket No. 17-108 (draft released Nov. 22, 2017). https://goo.gl/i3kmJE.

6. In addition to the Constitutional limit on judicial review to actual cases and controversies (U.S. Const. art. III, § 2), the judicial review of administrative agencies like the FTC is further constrained by the Administrative Procedure Act, Pub. L. No. 79-404, § 10, 60 Stat. 243 (codified at 5 U.S.C. § 706). See also *Chevron U.S.A. Inc. v. Nat. Res. Def. Council*, 467 U.S. 837, pp. 842–45 (1984).

7. See, e.g., U.S. House of Representatives, Energy & Commerce Committee, "Full Committee Advances Bills to Modernize the FTC and Put #InnovationFirst," Press Release, Jul. 14, 2016. https://goo.gl/kSR1Nj. For a detailed review of the legislative proposals, see, Berin Szóka and Geoffrey A. Manne, "The Federal Trade Commission: Restoring Congressional Oversight of the Second National Legislature—An Analysis of Proposed Legislation" FTC Technology and Reform Project, May 2016. https://goo.gl/36K7hM.

scope of this study,[8] which instead seeks to focus specifically on the FTC's abuse of consent decrees and the marked benefits that would be reaped if Congress were to circumscribe their use. Such an action would generate significant benefits for the regulatory environment as a whole because litigation of cases drives evolution and development of the law over time, and thus provides increased certainty for both industry and consumers about how the FTC's broad standards apply in different circumstances.[9]

## CURRENT FTC PROCESS ISSUES

The common law approach of case-by-case adjudication is far better at providing certainty than industry-wide rulemakings in areas that are undergoing rapid innovation and disruption to existing technologies and business models. This is because rules quickly become outdated and either ineffective or counterproductive as a result. However, the FTC's shift away from rulemaking and formal adjudication and toward consent decrees and informal guidance has all but nullified the benefits of this approach. Most notably, it has substantially reduced the level of judicial oversight over the FTC's actions.[10] It has also greatly reduced the level of guidance provided to both industry and consumers on how the agency's broad standards in Section Five of the FTC Act would apply in a given situation.[11]

While consent decrees may be in the best interest of the FTC and the party under investigation, they ultimately reduce guidance and stunt the development of appropriate and evolving legal standards. This harms consumer welfare and economic growth. Accordingly, the following sections describe the benefits of using case-by-case adjudication and common law over industry-wide rulemaking, and then explain how the FTC has recently deviated from that approach in a critical way through its abuse of consent decrees.

### Rulemaking vs. case-by-case adjudication

The FTC has authority to pursue its mission to protect consumers and competition through the use of either industry-wide rulemaking[12] or case-by-case adjudication.[13] It also has discretion to choose how to exercise that authority in any given circumstance.[14] However, there are situations in which case-by-case adjudication is clearly preferable to rulemaking, as explained by Justice Frank Murphy in the *SEC v. Chenery Corp.* (1947) opinion:

> Problems may arise in a case which the administrative agency could not reasonably foresee, problems which must be solved despite the absence of a relevant general rule. Or the agency may not have had sufficient experience with a particular problem to warrant rigidifying its tentative judgment into a hard and fast rule. Or the problem may be so specialized and varying in nature as to be impossible of capture within the boundaries of a general rule. In those situations, the agency must retain power to deal with the problems on a case-to-case basis if the administrative process is to be effective. There is thus a very definite place for the case-by-case evolution of statutory standards.[15]

Such a discussion illustrates that industry-wide rulemaking is at times imprudent—when the agency lacks "sufficient experience with a particular problem"—and at other times infeasible—when a problem is "so specialized and varying in nature as to be impossible of capture within the boundaries of a general rule."

The FTC has confronted both of these situations in the past. For example, it encountered the first in the 1970s when, under pressure from parents concerned about the health and wellbeing of their children, the Commission hastily proposed industry-wide rules that prohibited all children's advertising on television, which Congress later deemed to be an inappropriate use of the Commission's authority.[16] This fiasco resulted in a temporary shutdown of the Commission and legislative checks that terminated the rulemaking on children's advertising, eliminated the FTC's rulemaking authority in that area and imposed new procedural checks on its rulemaking authority across the board.[17]

This marked a major change in FTC process, as Congress forced it to rely more heavily upon case-by-case adjudication. Since then, the Commission has issued rules in specific areas that Congress has identified as requiring spe-

8. For excellent holistic takes on FTC reform, see, e.g., William E. Kovacic, *The Federal Trade Commission at 100: Into Our 2nd Century—The Continuing Pursuit of Better Practices*, U.S. Federal Trade Commission, January 2009. https://goo.gl/z6YjGV; and Berin Szóka & Graham Owens, "FTC Stakeholder Perspectives: Reform Proposals to Improve Fairness, Innovation, and Consumer Welfare," Testimony of TechFreedom at a Hearing Before the Subcommittee on Consumer Protection, Product Safety, Insurance, and Data Security of the U.S. Senate Committee on Commerce, Science, & Transportation, Sept. 26, 2017. https://goo.gl/tN9xKR.

9. See, e.g., Justin (Gus) Hurwitz, "Data Security and the FTC's UnCommon Law," *Iowa Law Review* 101:3 (2016), 980–88. https://goo.gl/pP6tAf.

10. See, e.g., Hurwitz, 980–88.

11. Federal Trade Commission Act, Pub. L. No. 63-203, § 5, 38 Stat. 719 (1914) (codified at 15. U.S.C. § 45). Section Five of the FTC Act declares unlawful and empowers the FTC to police all "unfair methods of competition" and "unfair or deceptive acts or practices."

12. See 15 U.S.C. § 57a(a).

13. See 15 U.S.C. § 45(b).

14. See *SEC v. Chenery Corp.*, 332 U.S. 194, p. 203 (1947).

15. Ibid., pp. 202–03.

16. See, e.g., Beales; and Mary L. Azcuenaga, "FTC Rulemaking: Harnessing Fire," Federal Trade Commissioner's Remarks Before the Society of Consumer Affairs Professionals in Business SOCAP Meeting, Sept. 12, 1985. https://goo.gl/pwM2xm.

17. See FTC Improvements Act of 1980, Pub. L. No. 96-252, §§ 7–11, 94 Stat. 374, 376 (1980) (codified at 15 U.S.C. § 57a).

cial attention,[18] but it has otherwise refrained from issuing industry-wide rules. Instead, it has used case-by-case adjudication, especially in innovative and dynamic areas like privacy and data security, which are practically "impossible of capture within the boundaries of a general rule."[19] Thus, it seems as though the FTC has learned the lesson of its previous overreach and has refrained from rulemaking in areas that are either unsuited to rules or where it lacks adequate understanding to promulgate effective ones. However, there are still significant issues with the FTC's current process of case-by-case adjudication.

## (Un)common law at the FTC

While commendable, particularly in dynamic industries with rapid innovation cycles, the FTC's shift toward greater reliance on case-by-case adjudication has significantly deviated from the true common law approach that Congress intended it to use in one critical way.[20] Specifically, rather than to litigate individual cases and produce binding precedent that industries can rely on prospectively for the purposes of compliance or business planning, the Commission has instead settled almost all of its cases via consent decrees. However, these produce no formal guidance, as they are never reviewed by an independent judge. By one account, over the past two decades the FTC has settled nearly three-quarters of its enforcement actions (1,524 out of 2,092) in this manner—without any adjudication or judicial oversight whatsoever.[21]

Such a practice lacks the key features that make true common law such an effective steward of liberty and driver of economic growth[22] and for this reason, commenters have derisively referred to it as "un-common law"[23] or the "common law of consent decrees."[24] Since 2002, the FTC has brought over 60 data security cases,[25] but it is still entirely unclear what level of data security constitutes an "unfair" practice under Section Five, as almost all of those cases ended in unadjudicated consent decrees. Only three companies have even been willing to challenge the FTC in a data security case, and no court has yet considered the question of whether the agency's complete reliance on informal guidance has given industry enough ability to comport with constitutional due process.[26] This is particularly concerning given the increasing importance of data security practices to economic security and growth.

It is certainly true that if the Commission were to litigate more and settle less, it would encounter more judicial setbacks—when attempts to extend precedent and prove a violation are rebuffed—especially in developing areas like privacy, data security and broadband regulation. However, such losses are actually quite beneficial for the health of the legal system as a whole. After all, the Commission's defeats in court can clarify the scope and boundaries of existing law, giving certainty to industry about how to conform their business practices. Formal adjudications and the judicial opinions they necessitate can also lay the groundwork for a future court to extend legal precedent to cover a new area or overturn existing precedent that no longer makes sense. In this way, the common law approach to case-by-case adjudication produces gradual evolution of legal standards over time, providing stability and predictability in the law's operation.[27]

Moreover, the current system merely allows the FTC to maximize its own discretion and its ability to extract pro-consumer and pro-competitive concessions from parties under investigation. If particular commissioners were dedicated to reforming internal agency process, individuals at the FTC could end this precedent on their own. However, a reliance upon personality politics is inevitably uncertain and impermanent. After all, future FTC staff with different inclinations could simply undo whatever interpretations or internal rulemakings their predecessors had done. Similarly, if it loses one of its currently pending cases and more parties are emboldened to challenge the FTC's enforcements, such reforms might inevitably be forced upon the Commission by the courts. Such an outcome, however, is uncertain and may take years or even decades to materialize. What is truly necessary, then, is congressional action to reform the FTC's use of consent decrees, as the incentives within the current legal framework all favor the status quo.

## Misaligned incentives and negative externalities

In the context of case-by-case adjudication, both the FTC and the company under investigation have strong incentives to settle an enforcement action and sign a consent decree. In so doing, a company generally agrees to undertake or refrain

18. See, e.g., Children's Online Privacy Protection Act of 1998, Pub. L. No. 105-227, 112 Stat. 2681-1 (codified at 15 U.S.C. §§ 6501 et seq.).

19. *Chenery Corp.* 332 U.S., p. 203; see also Bureau of Consumer Protection, "Privacy & Data Security Update: 2016," U.S. Federal Trade Commission, January 2017. https://goo.gl/8CaUgE.

20. See, e.g., Daniel A. Crane, "Debunking Humphrey's Executor," *George Washington University Law Review* 83:6 (November 2015), 1867. https://goo.gl/9UT3HP.

21. Ibid.

22. See, e.g., Paul G. Mahoney, "The Common Law and Economic Growth: Hayek Might Be Right," *The Journal of Legal Studies* 3:2 (June 2001), 503-25. https://goo.gl/3KNkuS.

23. See, e.g., Hurwitz. https://goo.gl/pP6tAf.

24. See, e.g., Berin Szóka and Geoffrey A. Manne, "The Second Century of the Federal Trade Commission," *Techdirt*, Sept. 26, 2013. https://goo.gl/SLkhM2.

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

26. See *FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015); *LabMD v. FTC*, No. 16-16270 (11th Cir. argued June 21, 2017); *FTC v. D-Link Corp.*, No. 3:17-cv-00039-JD (N.D. Cal. filed Jan. 05, 2017).

27. Hurwitz, 980. https://goo.gl/pP6tAf.

from certain practices—and without having to admit guilt or wrongdoing—in exchange for the FTC's termination of the enforcement action. From the company's perspective, this option is often desirable—even if a successful legal challenge could potentially exonerate the company from all liability—because of the substantial costs and uncertainty associated with litigation.[28] This incentive is even stronger because any challenge to the FTC's Civil Investigative Demands ("CIDs")—the equivalent of discovery requests—immediately publicizes the dispute, likely harming the company's reputation.[29] To comply with the CIDs and settle disputes via consent decree allows a company not only to avoid the admission of liability, but also to plan the release of the decree to correspond with announcements for various other pro-consumer or pro-competitive benefits, like individual refunds or the launch of new programs.[30] This type of strategic news bundling has been found to offset significantly the expected losses to stock market value that would otherwise be expected.[31] For these reasons, it is entirely reasonable for a company to utilize such a strategy in the context of FTC enforcements even when a legal challenge might be successful.

Likewise, from the FTC's perspective, to settle an enforcement action via consent decree is also an attractive option. Not only does it allow the Commission to avoid any potential embarrassment from pursuing a case that is ultimately unsuccessful,[32] it also enables it to enforce bigger penalties and extract greater concessions from the party under investigation than it could otherwise do under the law. The Commission's enforcement tools are strictly limited in adjudications,[33] but consent decrees allow for fines, injunctions, decades-long monitoring programs and essentially any other remedy to which the party under investigation is willing to agree.[34]

In view of the foregoing, it is easy to see why both the FTC and companies under its investigation would prefer to resolve disputes in this manner. However, as has been demonstrated, such a method provides no formal guidance to industry on whether or how certain practices violate the law, which is the true hallmark of the common law's evolutionary approach.[35] Further, since the benefit thereof has been described as a positive externality,[36] to work around it in favor of consent decrees should be viewed as a negative one. Accordingly, Congress should use its legislative capacity to internalize this negative externality by forcing the FTC to settle less and litigate more in order to ensure that consumers and competition reap the benefits associated with the true common law approach.

## RESTORING A TRUE COMMON LAW APPROACH

There are those who defend the FTC's use of consent decrees,[37] and some who believe it is functionally equivalent to a common law,[38] but a growing body of scholarly research recognizes the problems it causes.[39] In view of this, there have been several legislative changes proposed to address these problems, and these proposals have substantial merit. For example, to limit the maximum term of consent decrees[40] and/or to require them to be justified by an economic analysis that demonstrates that the public-interest benefits outweigh the costs would both make marginal differences.[41] From the FTC's perspective, such changes would make consent decrees less attractive because their scope would be more limited and the agency would be required to provide more detailed explanations for the consent decrees it does issue. This would encourage the Commission to settle less and litigate more. However, such measures still would not ensure that the FTC litigates more and generates more formal guidance going forward. Thus, while these proposed reforms would significantly curb the abuse of consent decrees at the FTC, they would arguably not go far enough.

To restore the true common law approach to FTC process and deliver the substantial benefits to consumer welfare and economic growth that come with it, Congress should simply prohibit the Commission from using consent decrees to settle enforcement actions unless the party admits liability. Since neither the Commission nor Congress can force

28. See, e.g., Hurwitz, 986.

29. See, e.g., "A Brief Overview of the Federal Trade Commission's Investigative and Law Enforcement Authority," U.S. Federal Trade Commission, July 2008. https://goo.gl/g85hAQ.

30. See, e.g., U.S. Federal Trade Commission, "Uber Settles FTC Allegations that it Made Deceptive Privacy and Data Security Claims," Press Release, Aug. 15, 2017. https://goo.gl/JixKH7.

31. See, e.g., Sebastien Gay, "Strategic News Bundling and Privacy Breach Disclosures," Aug. 21, 2015. https://goo.gl/GC2p6E.

32. Some might consider the time and effort spent pursuing a case that is ultimately unsuccessful to be wasteful, but the development of the law is itself a public good. For this reason, even bringing cases that are unsuccessful from the FTC's perspective may actually be a very good use of agency resources.

33. For example, the maximum civil penalty the FTC can seek for violations of Section Five is $40,654 per day for continuing violations. See U.S. Federal Trade Commission, "FTC Raises Civil Penalty Maximum to Account for Inflation," Press Release, June 29, 2016. https://goo.gl/yjtioJ.

34. See, e.g., Geoffrey A. Manne, "Federal Intrusion: Too Many Apps for That," *The Wall Street Journal*, Sept. 16, 2014. https://goo.gl/uU3FZW.

35. Hurwitz, 980. https://goo.gl/pP6tAf.

36. See, e.g., Ibid., 983.

37. See, e.g., Deborah L. Feinstein, "The Significance of Consent Decrees in the Federal Trade Commission's Competition Enforcement Efforts," Remarks of the Director of the Bureau of Competition of the U.S. Federal Trade Commission, Sept. 17, 2013. https://goo.gl/gCHjUZ.

38. See, e.g., Daniel J. Solove & Woodrow Hartzog, "The FTC and the New Common Law of Privacy," *Columbia Law Review* 114 (2014), 583. https://goo.gl/96DM9L.

39. See, e.g., Douglas H. Ginsburg and Joshua D. Wright, "Antitrust Settlements: The Culture of Consent," *Bill Kovacic Liber Amicorum*, Feb. 28, 2013. https://goo.gl/ieCFuJ; and Hurwitz. https://goo.gl/pP6tAf.

40. See, e.g., Szóka and Manne, 75–78. https://goo.gl/SLkhM2.

41. Ibid., 48–53.

companies to challenge legal actions against their will and because settlements are quicker and often less costly than litigation, to settle individual cases should still be permissible. However, this should only be allowed if the resulting settlements include an admission of liability for at least one of the charges, and an explanation of how the underlying conduct violated the law. Thus, for example, if the Commission alleged multiple violations of Section Five under different legal theories—say, by claiming both that a company's privacy practices were "unfair" and that its privacy policy describing such practices was "deceptive"[42]—it would be permissible for the Commission to drop the unfairness charge if the company admits liability for the deception. Effectively, this would make the FTC's consent decrees operate much like plea bargains in the criminal justice system. The resulting decrees may not be immediately subject to judicial review, but as formal FTC orders they would still establish binding precedent that could not be arbitrarily overturned by the Commission going forward.[43] Thus, to require consent decrees to contain both (1) an admission of liability on the part of the company under investigation, and (2) the FTC's explanation of how the underlying conduct violates the law, would produce even more binding precedent that can further drive development of the law and reduce industry uncertainty.

Additionally, limitations on the FTC's use of consent decrees could be combined with stronger authority, additional remedies and reforms to its judicial operations. For example, the statutory maximum for civil penalties could be changed from an absolute figure (i.e., a dollar amount) to a relative figure (e.g., some percentage of business revenues or profits).[44] This would give the Commission even greater incentive and ability to pursue formal adjudication and establish binding precedent to drive evolution of the law.[45] It would also ensure the Commission has adequate punishments available to penalize bad actors, regardless of how big or powerful they may be.

Congress could also consider hiring more administrative law judges (ALJs) to staff the FTC and hear cases within the agency.[46] Many scholars have criticized the FTC's use of administrative litigation,[47] but it can often provide quicker and cheaper resolution of legal disputes than the traditional court. Further, parties always have the right to appeal their claim in the traditional manner if they are unsatisfied with the determination of the administrative law judge. If there are lingering concerns over agency bias, Congress could also provide companies with the right to remove cases from the administrative litigation process during the initial trial phase, rather than having to wait for appeal—perhaps based on some showing of need or convenience.

FTC staff would likely resist these changes, preferring instead to maintain their vast discretion to resolve enforcement actions however they wish. From an institutional perspective, however, it is perfectly reasonable to restrict the FTC's use of consent decrees and force it to rely more upon formal adjudication. The benefits of the common law approach are well established, and Congress has already made clear that the FTC should use its broad authority to police unfair competition and protect consumers on a case-by-case basis. However, the FTC's overuse of consent decrees is harmful to both consumers, industry and the proper functioning of the law.

## CONCLUSION

During its more than a century-long existence, the FTC has been reformed many times and it will continue to change and evolve. Many of the changes to the FTC in recent years have been positive, but some have also been decidedly negative. In particular, the reliance on informal adjudication and abuse of consent decrees has led to a dearth of legal precedent and formal guidance, and this has generated substantial regulatory uncertainty.

These problems are unlikely to resolve themselves, as they are the result of the current incentive structures within the agency itself. Thus, Congress should enact a handful of simple reforms to the FTC's process that will substantially improve regulatory and enforcement outcomes for both consumers and competition. With these process reforms in place, the agency will finally be ready to tackle the vital competition and consumer protection issues of the 21st century.


### 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).


42. 15 U.S.C. § 45.

43. See, e.g., *FCC v. Fox Television Stations*, 132 S.Ct. 2307 (2012).

44. "FTC Raises Civil Penalty Maximum to Account for Inflation." https://goo.gl/yjtioJ.

45. See Maureen K. Ohlhausen, "Administrative Litigation at the FTC: Effective Tool for Developing the Law or Rubber Stamp?", *Journal of Competition Law & Economics* 12 (2016), 623. https://goo.gl/yWfQ6Z.

46. The FTC currently has only one ALJ, Chief Administrative Law Judge D. Michael Chappell. See Office of Administrative Law Judges, "D. Michael Chappell, Chief Administrative Law Judge, U.S. Federal Trade Commission, 2017. https://goo.gl/fqVDi6.

47. See, e.g., Joshua D. Wright, "Judging Antitrust," Remarks of the Commissioner of the Federal Trade Commission: Global Antitrust Institute Invitational Moot Court Competition, Feb. 21, 2015. https://goo.gl/9HPBvX.

OPINION

# A Positive Agenda for the New FTC

BY **TOM STRUBLE**
February 14, 2018

Today, the U.S. Senate's Committee on Commerce, Science and Transportation will convene a hearing to review President Donald Trump's nominees to head the Federal Trade Commission: Joseph Simons, Noah Phillips, Christine Wilson and Rohit Chopra. For over a year, the FTC has had only two commissioners — Acting Chairman Maureen Ohlhausen, a Republican, and Commissioner Terrell McSweeny, a Democrat — which left it unable to pursue any cases that would split political opinion. Once the nominees are confirmed, though, our nation's chief competition and consumer-protection agency will once again be able to tackle the most difficult and controversial economic issues of our time.

With its broad jurisdiction and limited resources, the FTC must pick and choose its battles wisely, and we can expect it to hew closely to conservative economic thinking when setting its agenda. However, abstract notions of regulatory humility and cost-benefit analysis are difficult to sell to average American voters. Thus, instead of focusing on what it won't do, the new FTC should develop a positive agenda of steps it will take to improve itself and better protect both consumers and competition going forward. Here are three suggestions:

**Litigate More Privacy & Cybersecurity Cases**

Privacy and cybersecurity are vital to the modern economy. As chief regulator of both, the FTC has brought dozens of privacy and cybersecurity cases over the years, but almost all these cases were settled via unadjudicated consent decrees, which establish no binding precedent. Consent decrees and other types of informal guidance (reports, letters, etc.) are useful, but they are no substitute for binding legal precedent, which can be obtained only by going to court and litigating cases to their conclusion.

Run-of-the-mill cases should still be settled, but any time the FTC faces a novel issue or relies on an untested legal theory, it should go to court and see whether its actions pass muster. Recent cases like LabMD, Wyndham and D-Link are a step in the right direction, but the new FTC should go even further to clarify what privacy or cybersecurity practices qualify as "unfair" or "deceptive." Last year saw major breaches revealed at Equifax and Uber, and similar events will surely continue so long as the FTC leaves industry in the dark when it comes to regulatory compliance. The new FTC should right the ship, reform its processes and litigate more privacy and cybersecurity cases.

**Put Up or Shut Up on Net Neutrality**

The Federal Communications Commission's Restoring Internet Freedom order restored the FTC's jurisdiction over broadband, and the new FTC will have primary responsibility for policing any unfair discrimination or anticompetitive behavior online. The FTC is no stranger to net neutrality, having issued a fulsome 170-page report on the matter in 2007 and having brought recent complaints against both TracFone and AT&T for deceptive throttling. However, some still doubt whether the agency is up to the task. The new FTC needs to prove whether it can handle net neutrality — and whether broadband regulation should stay at the

FTC — or whether Congress will need to step in and shift net neutrality back to the FCC.

Many believe the FTC can handle net neutrality because harm to consumers or competition from any unfair blocking, throttling or prioritization would map directly onto the FTC's authority in Section 5, but this theory has not been fully tested. An enforcement action would be the only true test of the FTC's net neutrality chops. However, hosting a workshop and/or updating its 2007 report to give additional guidance (albeit informal) on how the agency's authority would apply in the net neutrality context would also help.

Additionally, the new FTC should consider bolstering its Office of Technology Research and Investigation with additional computer scientists and electrical engineers who specialize in telecom. The FTC and FCC currently have a memorandum of understanding for exchanging information and coordinating online consumer protection efforts, but getting expertise in-house will be vital to making broadband regulation at the FTC a long-term success.



## Look Beyond the Swamp

Shrinking government and repealing costly regulations has been a key pillar of the Trump administration, which can claim several victories from 2017. However, while the effort to "drain the swamp" has been focused mostly on Washington, D.C., cronyism and arbitrage

also persist at the state and local levels. Here, too, the FTC can do tremendous good.

The FTC has a long, proud history of protecting consumers and promoting competition at the state and local levels. Its Office of Policy Planning promotes competition with both advocacy filings and amicus briefs, and it has successfully challenged unfair state licensing laws in court. However, there's more that could be done, particularly to address the growing body of occupational licensing laws that unfairly restrict competition, limit personal mobility and otherwise harm consumers. Acting Chairman Ohlhausen established an Economic Liberty Task Force to investigate occupational licensure in various industries and its effects on competition and consumers. The new FTC should continue this important work going forward.

Whether it's challenging occupational licensing and other forms of incumbent protectionism, or simply offering guidance on how to promote competition in industries undergoing rapid change, the new FTC should look beyond the swamp and make a concerted effort to protect competition and consumers at the state and local levels.

*Tom Struble is the technology policy manager for the R Street Institute.*

Morning Consult welcomes op-ed submissions on policy, politics and business strategy in our coverage areas. Updated submission guidelines can be found here.

TECH

39 | R Street Institute



Free markets. Real solutions.

CONTENTS



R STREET POLICY STUDY NO. 133
March 2018

# POLICY APPROACHES TO THE ENCRYPTION DEBATE

Charles Duan, Arthur Rizer, Zach Graves and Mike Godwin

## INTRODUCTION

A fierce debate has been ongoing for many years over strong computer encryption of communications and data, which can both deliver security and privacy for individuals but also make it difficult for the intelligence and law enforcement communities to perform their surveillance and investigative duties. In particular, the question of whether encryption systems should be required to have a "backdoor" to give the government special access to encrypted information remains divisive.[1]

Views on the question seem diametrically opposed: law enforcement communities contend that crime and terror will reign if the government cannot read all encrypted messages and information; by contrast, companies, technologists and civil liberties advocates decry the devastation to individual rights and public security if strong encryption is compromised. These polarized views have left policymakers at an impasse.

However, such seemingly irreconcilable perspectives on either side of the debate arise primarily because encryption policy is treated as a thought experiment, often with oversimplified facts coupled with a great deal of certainty. For example, the most commonly employed hypothetical scenario involves the following: an encrypted message or communication that—if only the government were able read it—would reveal the secrets required to stop a deadly attack or to bring a terrorist to justice.

This resembles another famous thought experiment: the "ticking time bomb," where torturing a suspect is the guaranteed and only means to defuse the bomb.[2] While this latter conundrum has also generated volumes of polarized debate, its most pragmatic solution is one that can also be applied to the issue of encryption, which is to reject the hypothetical's frame. This requires the realization that the thought experiment's simplified assumptions are not consistent with reality, accompanied by a shifted focus onto real-world questions about whether and how actual systems might be implemented.

Consistent with this pragmatic analysis, we believe that the right approach to the encryption debate is to consider three questions that must be answered before any encryption backdoor could possibly be advisable: whether there is empirical

1. "*Don't Panic: Making Progress on the 'Going Dark' Debate*," Berkman Center for Internet and Society, Feb. 1, 2016, pp. 5–7. https://cyber.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf; "Decrypting the Encryption Debate: A Framework for Decision Makers," National Academy of Sciences, 2018, pp. 6–7. https://www.nap.edu/catalog/25010/decrypting-the-encryption-debate-a-framework-for-decision-makers.

2. See, e.g., Fritz Allhoff, "A Defense of Torture: Separation of Cases, Ticking Time-Bombs, and Moral Justification," International Journal of Applied Philosophy 19:2 (2005), p. 243. http://files.allhoff.org/research/A_Defense_of_Torture.pdf.

evidence of a need for and benefit of a backdoor; whether there is a satisfactory technical solution; and whether law and policy can implement that technical solution. In contrast to the purely theoretical nature of the issue currently, each of these is amenable to experimentation, evidence-based debate and thoughtful discussion. Nevertheless, given the facts known today, it is unlikely that the associated hurdles will be overcome. Moreover, it is nearly impossible to overcome them all. That said, there is at least a way forward if stakeholders are willing to explore the three-part, real-world framework of cost–benefit analysis, adversarial testing of technology and policy implementation.

Accordingly, the present study provides background on encryption, backdoors, the "going dark" problem and the current debate. It then reviews each of these three prongs, develops a portion of the analytical framework, applies the facts as known today, and identifies policy proposals and points of future study in order to advance the discussion past its current stalemate.

## ENCRYPTION: AN OVERVIEW

Encryption is a method by which a message or other information is converted by a mathematical process such that the original message can only be recovered with a "key," usually a numerical value that can undo the code.[3] For example, a simple form of encryption would be to systematically replace letters in a message with other letters. In this case, the encryption key would be the table of letter replacements.[4]

The purpose of modern encryption is largely twofold. First, it prevents eavesdroppers from listening in on private conversations. Second, it provides those participating with assurance that they are talking with the people they expect.[5] This makes modern encryption an important tool for numerous private applications. For example, e-commerce transactions are encrypted to prevent thieves from stealing credit card numbers. Email and cell phone calls are encrypted to stop eavesdropping, and data stored on computers and mobile devices are encrypted to prevent sensitive information from being accessed if those devices are lost or stolen.[6] Data encryption has thus become essential to basic economic life and societal participation, as it gives the public confidence to store and transmit personal and financial data on computer systems.

Perhaps more importantly, encryption is an important tool of free speech and individual liberty. Repressive governments often use surveillance of communications to keep tabs on their citizens and encryption can offer a degree of freedom from that surveillance.[7] As a recent United Nations Educational, Scientific and Cultural Organization (UNESCO) report explains, "restriction of the availability and effectiveness of encryption as such constitutes an interference with the freedom of expression and the right to privacy."[8]

The flipside of that individual liberty, however, is that encryption can be used to oppose government power, such as in military conflict against the nation, acts of terrorism or criminal behavior. As a result, governments have long had an interest in "breaking" encryption—that is, in applying various measures to obtain encryption keys or otherwise decipher encrypted messages. During the Second World War, for example, British computer scientist Alan Turing famously invented a mathematical engine that broke the German "Enigma" encryption.[9]

Encryption thus holds substantial value to individuals, but governments also see it as a threat that adversaries may deploy against the national interest. It is this tension that leads to the current debate over "going dark."

## THE "GOING DARK" PROBLEM AND THE BACKDOOR DEBATE

A term used in the law enforcement field, particularly by the Federal Bureau of Investigation, "going dark" refers to the process by which encryption or other techniques obscure information in ways that prevent the government from accessing it, even in situations wherein the government is otherwise authorized by law to do so.[10] With the increasing prevalence of encryption, the FBI has expressed a "fear of missing out" on preventable crimes or prosecutable criminals, arguing that it cannot access the necessary evidence.[11]

3. *Bernstein v. U.S. Dep't of Justice*, 176 F.3d 1132, 1137 (9th Cir. 1999).

4. Julius Caesar famously used this sort of encryption. See Suetonius, *De Vita Caesarum*, tr. J.C. Rolfe (William Heinemann: 1914), I, sec. 56. https://catalog.hathitrust.org/Record/001182041.

5. *Bernstein v. U.S. Dep't of Justice*, 176 F.3d 1137.

6. S. Kelly, "*Security Implications of Using the Data Encryption Standard (DES),*" Internet Engineering Task Force RFC 4772, pp. 7–8, Dec. 2006. https://www.rfc-editor.org/rfc/rfc4772.txt.

7. Andy Greenberg, "Encryption App 'Signal' Is Fighting Censorship with a Clever Workaround," *Wired*, Dec. 21, 2016. https://www.wired.com/2016/12/encryption-app-signal-fights-censorship-clever-workaround.

8. Wolfgang Schulz and Joris van Hoboken, "*Human Rights and Encryption*," UNESCO Series on Internet Freedom, 2016, p. 55. http://unesdoc.unesco.org/images/0024/002465/246527E.pdf.

9. "The Enigma of Alan Turing," *Central Intelligence Agency*, April 10, 2015. https://www.cia.gov/news-information/featured-story-archive/2015-featured-story-archive/the-enigma-of-alan-turing.html.

10. Testimony of Amy Hess, Executive Assistant Director, Federal Bureau of Investigation, Subcommittee on Information Technology of the House Committee on Oversight and Government Reform, "Encryption Technology and Potential U.S. Policy Responses," 114th Congress (GPO, 2015), p. 9. https://www.gpo.gov/fdsys/pkg/CHRG-114hhrg25879/pdf/CHRG-114hhrg25879.pdf.

11. James B. Comey, Director, Federal Bureau of Investigation, "Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?", Brookings Institution, Oct. 16, 2014. https://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course.

It is, of course, not novel to use encryption to thwart the prying eyes of government agents. Jefferson and Madison themselves encrypted their letters to prevent them from being read during the French Revolution.[12] Nevertheless, today's widespread adoption of encryption-enabled technology has led law enforcement to call vociferously for a technical solution to the problem of going dark.

The most commonly proposed solution is the installation of a "backdoor," or a generalized change to current encryption technologies that enables the government or law enforcement to read encrypted communications and stored data.[13] In 2015, for example, the FBI argued that it needs a "way to access encrypted systems and data," or else "many investigations could be at a dead end."[14] The problem, however, is that while there can be little objection to a theoretically perfect backdoor that only the government may access in permitted situations, no such perfect backdoor exists. Technology cannot inherently distinguish between good guys and bad guys, and thus any backdoor will open at least some possibility that hackers and rogue government officials will gain access.

Encryption backdoors are not a new idea within the federal government: There have been several historical examples of calls for—and even the successful installment of—backdoors in standard encryption systems, often at the behest of the National Security Agency. For example, the Data Encryption Standard (DES), which IBM developed in the 1970s with the NSA's input, has been alleged to include a form of backdoor—namely an encryption key size sufficiently small that "a $20 million machine can be built to break the proposed standard in about 12 hours of computation time."[15] The unsuccessful Clipper Chip proposal was another attempt to require a backdoor for government access.[16] And the Dual EC algorithm, adopted as part of federal encryption standards between 2006 and 2014, was widely suspected to have included one that gave the NSA a secret edge in guessing encryption keys.[17] This suspicion was confirmed by internal NSA documents later leaked by Edward Snowden.[18]

But the problem of going dark has attracted a great deal of recent attention, in part due to recent investigations of terrorist attacks involving encrypted cell phones,[19] and in part due to the introduction of default device encryption and new encryption services around 2014.[20] Indeed, as late as 2011 the FBI was not advocating for encryption backdoors. In fact, its representative testified to Congress that year that "[a]dressing the Going Dark problem does not require fundamental changes in encryption technology."[21] Today's narrative has shifted substantially. For example, this year, current FBI Director Christopher Wray called the need to redesign encryption-based systems to assist law enforcement "an urgent public safety issue."[22]

Debate over encryption backdoors is polarized. Law enforcement proponents that call for extensive access to encrypted data are firmly pitted against companies and civil society advocates who contend that any backdoor will fundamentally weaken technology, communications, the Internet and global competition.

Advocates on the law enforcement side have claimed that, with increasing prevalence of "default-on" encryption, to deny law enforcement a mechanism to access encrypted information will lead to more crimes going unsolved and further threats to public safety. James Comey, then-director of the FBI, remarked in 2014 that "encryption threatens to lead all of us to a very dark place."[23] Deputy Attorney General

12. John A. Fraser, III, "The Use of Encrypted, Coded and Secret Communications Is an 'Ancient Liberty' Protected by the United States Constitution," *Virginia Journal of Law and Technology* 2:1 (1997), p. 2. http://vjolt.org/wp-content/uploads/2017/Articles/vol2/issue/vol2_art2.html.

13. The term "backdoor" is used throughout only because it is the colloquial term currently used in policy discussions. See, e.g., John Leyden, "We Need to Talk About Mathematical Backdoors in Encryption Algorithms," *The Register*, Dec. 15, 2017. https://www.theregister.co.uk/2017/12/15/crypto_mathematical_backdoors. Other commentators have used phrases such as "extraordinary access" or "privileged access." But these are not necessarily preferable because they have other meanings in the information technology field. See, e.g., Sandra Henry-Stocker, "Unix: Controlling Privileged Access," *Network World*, July 28, 2014. https://www.networkworld.com/article/2696974/operating-systems/unix---controlling-privileged-access.html.

14. Testimony of Amy Hess, "Encryption Technology and Potential U.S. Policy Responses," p. 11. https://www.gpo.gov/fdsys/pkg/CHRG-114hhrg25879/pdf/CHRG-114hhrg25879.pdf.

15. Whitfield Diffie and Martin E. Hellman, "Exhaustive Cryptanalysis of the NBS Data Encryption Standard," *Computer*, June 1977, p. 74. https://stacks.stanford.edu/file/druid:kf335sp7778/kf335sp7778.pdf.

16. A. Michael Froomkin, "The Metaphor Is the Key: Cryptography, the Clipper Chip, and the Constitution," *University of Pennsylvania Law Review* 143:3 (1995), p. 709. http://scholarship.law.upenn.edu/penn_law_review/vol143/iss3/3.

17. Bruce Schneier, "Did NSA Put a Secret Backdoor in New Encryption Standard?", *Wired*, Nov. 15, 2007. https://www.wired.com/2007/11/securitymatters-1115.

18. Nicole Perlroth, "Government Announces Steps to Restore Confidence on Encryption Standards," *The New York Times*, Sept. 10, 2013. https://bits.blogs.nytimes.com/2013/09/10/government-announces-steps-to-restore-confidence-on-encryption-standards.

19. Ellen Nakashima, "FBI Paid Professional Hackers One-Time Fee to Crack San Bernardino iPhone," *The Washington Post*, April 12, 2016. https://www.washingtonpost.com/world/national-security/fbi-paid-professional-hackers-one-time-fee-to-crack-san-bernardino-iphone/2016/04/12/5397814a-00de-11e6-9d36-33d198ea26c5_story.html.

20. Apple and Google announced default encryption for their devices in 2014, and an encrypted communications app, Signal, was released the same year. See Joe Miller, "Google and Apple to Introduce Default Encryption," *BBC News*, Sept. 19, 2014. http://www.bbc.com/news/technology-29276955; and Andy Greenberg, "Your iPhone Can Finally Make Free, Encrypted Calls," *Wired*, July 29, 2014. https://www.wired.com/2014/07/free-encrypted-calling-finally-comes-to-the-iphone.

21. Testimony of Valerie Caproni, General Counsel, Federal Bureau of Investigation, Subcommittee on Crime, Terrorism and Homeland Security of the House Committee on the Judiciary, "Going Dark: Lawful Electronic Surveillance in the Face of New Technologies," 112th Congress (GPO, 2011), p. 12. http://judiciary.house.gov/_files/hearings/printers/112th/112-59_64581.pdf.

22. Christopher Wray, "Raising Our Game: Cyber Security in an Age of Digital Transformation," FBI International Conference on Cyber Security, Jan. 9, 2018. https://www.fbi.gov/news/speeches/raising-our-game-cyber-security-in-an-age-of-digital-transformation.

23. Comey. https://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course.

Rod Rosenstein has similarly warned: "Encrypted communications and devices pose the greatest threat to public safety when they are part of mass-market consumer devices and services that enable warrant-proof encryption by default."[24] Another FBI employee reportedly called Apple developers "jerks" and "evil geniuses" for making iPhone passwords more difficult to guess.[25]

The solution that law enforcement seeks has generally been a blanket obligation on software or device vendors to enable the government to retrieve unencrypted data or intercept unencrypted communications. The Manhattan District Attorney's Office has proposed federal legislation that requires smartphone and tablet manufacturers to render those devices "capable of being accessed by the designer in unencrypted form pursuant to a search warrant or other lawful authorization."[26] During his tenure as FBI director, Comey called instead for "a regulatory or legislative fix" to enable law enforcement to overcome encryption.

Denouncements of such proposals have been equally vigorous. In 2015, a group of fifteen computer scientists and security experts posited that encryption backdoors "are unworkable in practice, raise enormous legal and ethical questions, and would undo progress on security at a time when Internet vulnerabilities are causing extreme economic harm."[27] Cybersecurity experts have also warned that any encryption backdoor "may result in adverse collateral effects, affecting the competitiveness of American businesses and U.S. national security."[28] Representative Ted Lieu (a Stanford computer science graduate) has also quipped: "Creating a pathway for decryption only for good guys is technologically stupid. You just can't do that."[29]

Given such strong opinions about backdoors, opponents have largely expressed unwillingness to explore proposals on the subject. A 2015 letter signed by civil society organizations, companies, trade associations, and security and policy experts thus called on the Administration "to reject any proposal that U.S. companies deliberately weaken the security of their products."[30]

However, to a degree, such narrow, largely theoretical debates are oversimplifications. The question of whether we should or should not have backdoors for law enforcement must be predicated on a deliberate analysis of whether or not they are actually necessary and useful, technologically possible and/or implementable in the first place. These are practical questions about real-world systems, and more importantly they are amenable to evidence-based testing and discussion. Accordingly, the following sections analyze these three main questions that should be answered before any backdoor could be advisable.

## QUESTION ONE: IS A BACKDOOR NECESSARY OR USEFUL?

No backdoor should be forced upon encrypted systems unless the benefits outweigh the costs. The costs are well known and established in other literature and include risks to national security,[31] increased public exposure to thieves and hackers,[32] injury to economic and global competitiveness,[33] and diminishment of individual privacy and liberty.[34]

The benefits of a backdoor should also be quantifiable. For example, statistics can be produced on the number of crimes that go unsolved or criminals who are not prosecuted successfully because key evidence was available but remained encrypted. If that quantitative evidence were produced, policymakers would then be faced with the likely difficult task of balancing the costs and benefits.

### Lack of empirical evidence

As it stands, such evidence has not surfaced in the first place. The benefits of an encryption backdoor that proponents have

24. Rod J. Rosenstein, Deputy Attorney General, "Remarks at the U.S. Naval Academy," Oct. 10, 2017. https://www.justice.gov/opa/speech/deputy-attorney-general-rod-j-rosenstein-delivers-remarks-encryption-united-states-naval.

25. Lorenzo Franceschi-Bicchierai, "FBI Hacker Says Apple Are 'Jerks' and 'Evil Geniuses' for Encrypting iPhones," *Vice: Motherboard,* Jan. 10, 2018. https://motherboard.vice.com/en_us/article/59wkkk/fbi-hacker-says-apple-are-jerks-and-evil-geniuses-for-encrypting-iphones.

26. "Smartphone Encryption and Public Safety: An Update to the November 2015 Report," Manhattan District Attorney's Office, November 2016, p. 32. https://www.manhattanda.org/wp-content/themes/dany/files/Report%20on%20Smartphone%20Encryption%20and%20Public%20Safety:%20An%20Update.pdf.

27. Peter G. Neumann et al., "Keys Under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications," *Communications of the ACM 58:10* (October 2015), p. 1. http://www.csl.sri.com/users/neumann/cacm237.pdf.

28. "*The Ground Truth About Encryption and the Consequences of Extraordinary Access," The Chertoff Group,* 2016, p. 17. https://www.chertoffgroup.com/files/238024-282765.groundtruth.pdf.

29. "Encryption Technology and Potential U.S. Policy Responses," p. 69. https://www.gpo.gov/fdsys/pkg/CHRG-114hhrg25879/pdf/CHRG-114hhrg25879.pdf.

30. "Letter from civil society organizations, companies, trade associations, and security and policy experts, to President Barack Obama," May 19, 2015, p. 1. https://static.newamerica.org/attachments/3138--113/Encryption_Letter_to_Obama_final_051915.pdf.

31. See, e.g., Peter Swire and Kenesa Ahmad, "Encryption and Globalization," *Columbia Science and Technology Law Review* 13:2 (2012), pp. 454–57. http://stlr.org/volumes/volume-xiii-2011-2012/encryption-and-globalization.

32. See, e.g., Kevin Bankston, "The Numbers Don't Lie: How Smartphone Encryption Will Help Cops More Than It Hurts Them," *Slate*, Aug. 18, 2015. http://www.slate.com/articles/technology/future_tense/2015/08/default_smartphone_encryption_will_stop_more_crimes_than_it_permits.html. A study by security firm Symantec found that those who find lost phones almost always try to access personal information on those phones, which suggests that unencrypted and unlocked phones are vulnerable to information or identity theft. See "*The Symantec Smartphone Honey Stick Project," Symantec*, 2012, pp. 12–13. http://www.symantec.com/content/en/us/about/presskits/b-symantec-smartphone-honey-stick-project.en-us.pdf.

33. See, e.g., Swire and Ahmad, pp. 457–59. http://stlr.org/volumes/volume-xiii-2011-2012/encryption-and-globalization.

34. See, e.g., Froomkin, pp. 811–12. http://scholarship.law.upenn.edu/penn_law_review/vol143/iss3/3.

offered so far are currently only theoretical and are most often presented within the scenario of a hypothetical criminal or terrorist using secure lines and encrypted phones. Although there have been several anecdotal suggestions that encryption interferes with investigations or crime prevention, proponents of backdoors have not yet demonstrably quantified their need.

With respect to wiretaps, for example, encryption is responsible for thwarting law enforcement in a relatively small percentage of cases. The Administrative Office of the U.S. Courts produces an annual report of Title III wiretapping.[35] For 2016, it shows that out of 3,168 wiretaps conducted, encryption was encountered in only 125 instances, and could not be decrypted in 101 cases—only roughly 3.2% of all wiretaps.[36] Certainly the meaningfulness of that statistic is limited by self-selection bias (most investigators probably do not ask for court orders to wiretap likely encrypted information), but it does at least show that many wiretaps are successful and not rendered ineffective by encryption specifically.

Regarding encrypted devices such as smartphones, several law enforcement offices have reported large numbers of devices seized that "remain inaccessible due to default device encryption."[37] But conspicuously missing from these reports are indications of how many such devices were the linchpin of investigations, as opposed to merely being devices that were seized routinely but were ultimately unnecessary in view of other evidence. Recently, the Manhattan district attorney identified a handful of anecdotes that described investigations possibly blocked due to encryption (none of which, curiously, were within his jurisdiction),[38] but reliance on anecdotal evidence seems to imply that the statistics are just not there.

Indeed, the case most often cited in favor of the need for a backdoor is the San Bernardino shooting and attempted bombing on December 2, 2015.[39] While the FBI strenuously argued for a court order to compel Apple to build a backdoor to unlock an iPhone that belonged to one of the shooters,[40] soon thereafter, it withdrew its request. Instead, it hired an outside firm to exploit a security vulnerability in the phone to gain access.[41] This is a case, then, where a backdoor ultimately proved to be unnecessary.[42]

It appears that efforts to collect evidence in support of the need for a backdoor today are in the works: A joint partnership between the FBI and local law enforcement, the National Domestic Communications Assistance Center (NDCAC), is now operating a Statistics Collection Tool to collect example cases "where evidence in a smart phone is unattainable due to encryption, but could have been critical in solving cases."[43] Nevertheless, the evidence so far is certainly insufficient.

Such a conspicuous lack of evidence contrasts sharply with another debate over encryption. In 1994, Congress passed the Communications Assistance for Law Enforcement Act, which included a provision that required telecommunications providers to offer certain assistance to law enforcement in decrypting communications.[44] In the hearings that led to the passage of that law, the FBI was able to "presen[t] a variety of statistics and categories" including those "regarding the thwarting of investigations across federal law enforcement as well as state and local law enforcement,"[45] and the Government Accounting Office performed similar research.[46] This suggests that it is certainly possible for law enforcement to quantify their assertions of need, but in this case they have simply failed to do so.

## Legal restrictions

There is good reason to believe that law enforcement has not produced such evidence because a backdoor is, in fact, not useful—at least to the extent that the law would allow it to be used. The Fourth Amendment prohibits the federal

35. 18 U.S.C. § 2519(3). https://www.law.cornell.edu/uscode/text/18/2519.

36. "Wiretap Report 2016," Administrative Office of the United States Courts, Dec. 31, 2016. http://www.uscourts.gov/statistics-reports/wiretap-report-2016.

37. "Smartphone Encryption and Public Safety," pp. 8–9. https://www.manhattanda.org/wp-content/themes/dany/files/Report%20on%20Smartphone%20Encryption%20and%20Public%20Safety:%20An%20Update.pdf; and Rosenstein. https://www.justice.gov/opa/speech/deputy-attorney-general-rod-j-rosenstein-delivers-remarks-encryption-united-states-naval. However, some have questioned the accuracy of these numbers. See, e.g., Marcy Wheeler, "Is FBI Still Fluffing Its Encryption Numbers?", *Emptywheel*, Nov. 11, 2016. https://www.emptywheel.net/2016/11/11/fbi-still-fluffing-encryption-numbers.

38. "Smartphone Encryption and Public Safety," pp. 10–11. https://www.manhattanda.org/wp-content/themes/dany/files/Report%20on%20Smartphone%20Encryption%20and%20Public%20Safety:%20An%20Update.pdf.

39. Ibid., pp. 6–7.

40. "Government's Ex Parte Application for Order Compelling Apple Inc. to Assist Agents in Search," *In re Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS3000*, No. 5:16-cm-10 (C.D. Cal. Feb. 16, 2016), p. 3. https://epic.org/amicus/crypto/apple/In-re-Apple-FBI-AWA-Application.pdf.

41. "Government's Ex Parte Application for a Continuance," *In re Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS3000*, No. 5:16-cm-10 (Mar. 21, 2016). https://epic.org/amicus/crypto/apple/191-FBI-Motion-to-Vacate-Hearing.pdf.

42. Certainly, the vulnerability exploitation avenue was less efficient, but it is hard to imagine that efficiency concerns alone could justify an encryption backdoor.

43. "We Need Examples of Cases Hindered By 'Going Dark,'" *Prosecutors' Center for Excellence*, April 4, 2017. http://pceinc.org/need-examples-cases-hindered-going-dark; "Smartphone Encryption and Public Safety," pp. 10–11. https://www.manhattanda.org/wp-content/themes/dany/files/Report%20on%20Smartphone%20Encryption%20and%20Public%20Safety:%20An%20Update.pdf.

44. 47 U.S.C. § 1002(b)(3). https://www.law.cornell.edu/uscode/text/47/1002.

45. Carrie Cordero, "Weighing in on the Encryption and 'Going Dark' Debate," *Lawfare*, Dec. 4, 2014. https://lawfareblog.com/weighing-encryption-and-going-dark-debate.

46. Ibid.

government and states from conducting "unreasonable searches and seizures,"[47] and courts have interpreted that provision to strongly protect a citizen's "reasonable expectation of privacy," especially in private communications and information in private possession.[48] Furthermore, the Fourth Amendment's requirement that warrants must "particularly describ[e] the place to be searched, and the persons or things to be seized"[49] prohibits "general warrants" that would authorize "searches in any place, for any thing,"[50] and thus likely limits the government's power to conduct mass surveillance in the first place.[51]

Even information not protected under the Fourth Amendment, such as a financial transaction voluntarily disclosed to a third party,[52] is not open to all government inspection because federal statutes impose further limits. When gathering foreign intelligence, for example, the Foreign Intelligence Surveillance Act (FISA) of 1978 may require the government "to minimize the acquisition and retention, and prohibit the dissemination" of domestic parties' communications or information in several situations.[53] The USA Freedom Act of 2015 imposes further limits on long-term government collection of "call detail records" and certain mass wiretapping.[54] Title III of the Omnibus Crime Control and Safe Streets Act of 1968 prohibits the government from wiretapping any "wire or oral communication" without consent or prior judicial authorization, and requires the government to make a high showing of the need for wiretapping.[55] The Electronic Communications Privacy Act of 1986 later extended Title III and its limitations to wiretapping of electronic communications,[56] and further imposed limits on law enforcement access to emails or other data stored on a "remote computing service" (a cloud service, in today's nomenclature).[57]

Such an intricate tapestry of rules regarding government surveillance is important because it shows many circumstances where an encryption backdoor could not be used, even if one was present.

## Efficacy and utility of already available technology

Within the confines of this legal framework, the government has access to a wealth of information through alternate investigative means—even without an encryption backdoor. Indeed, some commentators have called today the "golden age of surveillance."[58] And, in the numerous cases where these other avenues are sufficient for the needs of the justice and intelligence systems, a backdoor would be duplicative and thus unnecessary.[59]

Today, much information is unencrypted and available to law enforcement already. For example, metadata, or the "data about data" that often travels with encrypted information,[60] is largely unencrypted and can reveal location information,[61] unique identities of individuals,[62] telephone numbers dialed,[63] subject lines of emails,[64] identities of confederates

47. U.S. Constitution, Amendment IV; *Mapp v. Ohio*, 367 U.S. 643, 655 (1961).

48. *Katz v. United States*, 389 U.S. 347, 360 (1967) (Harlan, J., concurring); *United States v. Jones*, 132 S. Ct. 945, 949 (2012).

49. U.S. Constitution, Amendment IV.

50. *Boyd v. United States*, 116 U.S. 616, 641 (1886) (Miller, J., concurring); *Stanford v. Texas*, 379 U.S. 476, 481 (1965).

51. Richard A. Posner, "Privacy, Surveillance, and the Law," The *University of Chicago Law Review* 75:1 (2008), p. 254. https://chicagounbound.uchicago.edu/uclrev/vol75/iss1/11; Robert Bloom and William J. Dunn, "The Constitutional Infirmity of Warrantless NSA Surveillance: The Abuse of Presidential Power and the Injury to the Fourth Amendment," *William and Mary Bill of Rights Journal* 15 (2006), pp. 191–92. http://lawdigitalcommons.bc.edu/lsfp/163.

52. *United States v. Miller*, 425 U.S. 435, 443 (1976). The Supreme Court is currently considering a case that may limit this so-called third-party doctrine. See *United States v. Carpenter*, 137 S. Ct. 2211 (2017) (mem).

53. Foreign Intelligence Surveillance Act of 1978 (FISA), Pub. L. No. 95-511, § 101(h), 92 Stat. 1783 (codified at 50 U.S.C. §§ 1801–1885c). https://www.gpo.gov/fdsys/granule/STATUTE-92/STATUTE-92-Pg1783/content-detail.html. See also, Ibid., § 102(a)(1)(C); § 104(a)(5).

54. USA Freedom Act of 2015, Pub. L. No. 114-23, §§ 101(a)(3), 103 & 201, 129 Stat. 268. https://www.gpo.gov/fdsys/pkg/PLAW-114publ23/content-detail.html.

55. Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, § 802, § 2511(1)(a), (c), 82 Stat. 197. https://www.gpo.gov/fdsys/granule/STATUTE-82/STATUTE-82-Pg197/content-detail.html. See also, Ibid., § 2518(3)(c); § 2516.

56. Electronic Communications Privacy Act of 1986 (ECPA), Pub. L. No. 99-508, § 101(c), 100 Stat. 1848. https://www.gpo.gov/fdsys/granule/STATUTE-100/STATUTE-100-Pg1848/content-detail.html.

57.Ibid., § 201, § 2703.

58. Peter Swire, "The Golden Age of Surveillance," *Slate*, July 15, 2015. http://www.slate.com/articles/technology/future_tense/2015/07/encryption_back_doors_aren_t_necessary_we_re_already_in_a_golden_age_of.html.

59. See, e.g., "*Don't Panic: Making Progress on the 'Going Dark' Debate,*" pp. 9–10. https://cyber.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf.

60. See, e.g., Elizabeth W. King, "The Ethics of Mining for Metadata Outside of Formal Discovery," *Penn State Law Review* 113:3 (2009), pp. 805–07. http://www.pennstatelawreview.org/print-issues/articles/the-ethics-of-mining-for-metadata-outside-of-formal-discovery.

61. *See, e.g., United States v. Jones*, 132 S. Ct. 945, 949 (2012).

62. See, e.g., Peter Eckersley, "How Unique Is Your Web Browser?", *Proceedings of the International Conference on Privacy Enhancing Technologies* 10 (2010), p. 1. https://panopticlick.eff.org/static/browser-uniqueness.pdf.

63. *See, e.g., ACLU v. Clapper*, 785 F.3d 787, 793 (2d Cir. 2015).

64. See, e.g., Tim Worstall, "Why Email Can Never Be Truly Secure: It's the Metadata," *Forbes*, Aug. 18, 2013. https://www.forbes.com/sites/timworstall/2013/08/18/why-email-can-never-be-truly-secure-its-the-metadata.

or accomplices[65] and more.[66] "Side channel" information,[67] such as timing and rates of communications, are also observable by law enforcement and can uncover equally important information[68]—potentially enough even to decipher passwords.[69] All of this is so revealing about a person that it "reflects a wealth of detail about her familial, political, professional, religious, and sexual associations."[70]

Furthermore, the government already has several ways to overcome encryption through legal or technological processes.[71] For example, it can use existing security vulnerabilities to hack into devices or communication systems and retrieve information, as it apparently did with the locked iPhone identified after the San Bernardino shooting.[72] The government can almost certainly compel a suspect to unlock a device using biometrics such as a fingerprint scanner,[73] and according to some courts, may be able to compel him or her to enter a decryption password (although most courts would hold that to be a violation of the Fifth Amendment right against self-incrimination).[74]

Most importantly, the government often has access to third-party devices, services and systems that can help to obtain digital evidence. Cloud storage providers generally do not encrypt data in ways they cannot access,[75] so the government can use a variety of legal tools to gain entry.[76] Telecommunications providers, including broadband and voice-over-IP services, already must offer law enforcement assistance in decrypting communications in certain situations.[77] And Internet-of-Things devices, such as in-home cameras and wearable fitness trackers, are notably vulnerable to hacking and thus can be commandeered or otherwise accessed by government, which renders those devices a "potentially bountiful surveillance platform."[78]

Above all, the investigative strategies outlined raise important policy questions of their own as to how their use should be regulated.[79] However, law enforcement is likely not using these strategies to their fullest extent. Making better use of these already available "workarounds" would further reduce the number of cases where a backdoor would be necessary. Indeed, it is telling that multiple intelligence officials have called the need for encryption backdoors "overblown," arguing instead that skilled investigators "will develop technologies and techniques to meet their legitimate mission goals"—with or without backdoors.[80]

Moreover, the sophistication of criminals or terrorists sometimes requires the use of a workaround as opposed to a backdoor. This is because do-it-yourself encryption techniques are readily available on the Internet, and thus are essentially impervious to the latter. For example, the convicted

65. See, e.g., "The Golden Age of Surveillance." http://www.slate.com/articles/technology/future_tense/2015/07/encryption_back_doors_aren_t_necessary_we_re_already_in_a_golden_age_of.html.

66. See, e.g., Jane Mayer, "What's the Matter with Metadata?", *The New Yorker*, June 6, 2013. https://www.newyorker.com/news/news-desk/whats-the-matter-with-metadata.

67. Formally called a "side-channel attack," such a method is a strategy for breaking encryption or otherwise reading a message not by obtaining the message content, but rather by observing external environment variables, such as the timing of message transmissions or electromagnetic radiation emissions from wires. See, e.g., François-Xavier Standaert et al., "A Unified Framework for the Analysis of Side-Channel Key Recovery Attacks," *Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques* 28 (2009), p. 446. https://link.springer.com/content/pdf/10.1007/978-3-642-01001-9_26.pdf.

68. *See, e.g., Kyllo v. United States*, 533 U.S. 27, 38 (2001).

69. See, e.g., Dawn Xiaodong Song et al., "Timing Analysis of Keystrokes and Timing Attacks on SSH," *Proceedings of the Conference on USENIX Security Symposium* 10, Aug. 13-17, 2001. https://www.usenix.org/legacy/events/sec01/full_papers/song/song.pdf.

70. *United States v. Jones*, 132 S. Ct. 945, 955 (2012) (Sotomayor, J., concurring) (citing *People v. Weaver*, 12 N.Y.3d 433, 441–42 [2009]); see also *United States v. Carpenter*, 137 S. Ct. 2211 (2017) (mem).

71. Orin S. Kerr and Bruce Schneier, "Encryption Workarounds," *Georgetown Law Journal* 106 (forthcoming 2018), pp. 5–29. https://dx.doi.org/10.2139/ssrn.2938033.

72. Joseph Cox, "Confirmed: Carnegie Mellon University Attacked Tor, Was Subpoenaed By Feds," *Vice: Motherboard*, Feb. 24, 2016 https://motherboard.vice.com/en_us/article/d7yp5a/carnegie-mellon-university-attacked-tor-was-subpoenaed-by-feds.

73. *See, e.g., United States v. Dionisio*, 410 U.S. 1, 5–6 (1973).

74. See, e.g., *In re Grand Jury Subpoena Duces Tecum*, 670 F.3d 1335, 1346 (11th Cir. 2012); *United States v. Apple MacPro Computer*, 851 F.3d 238, 247–48 (3d Cir. 2017); and Orin Kerr, "The Fifth Amendment Limits on Forced Decryption and Applying the 'Foregone Conclusion' Doctrine," *The Washington Post*, June 7, 2016. https://www.washingtonpost.com/news/volokh-conspiracy/wp/2016/06/07/the-fifth-amendment-limits-on-forced-decryption-and-applying-the-foregone-conclusion-doctrine.

75. Christopher Soghoian, "Caught in the Cloud: Privacy, Encryption, and Government Back Doors in the Web 2.0 Era," *Journal on Telecommunications and High Technology Law* 8:2 (2010), pp. 392–96. http://www.jthtl.org/content/articles/V8I2/JTHTLv8i2_Soghoian.PDF.

76. See, e.g., Fed. R. Crim. P. 17(c)(1); All Writs Act, 28 U.S.C. § 1651, applied in *United States v. N.Y. Tel. Co.*, 434 U.S. 159, 172 (1977). https://www.law.cornell.edu/uscode/text/28/1651. Obviously, the government must "fully satisfy the statute's threshold requirements" for a legal procedure such as the All Writs Act to apply. See *In re Order Requiring Apple, Inc. to Assist in the Execution of a Search Warrant Issued by this Court*, 149 F. Supp. 3d 341, 351 (E.D.N.Y. 2016).

77. See Communications Assistance for Law Enforcement Act (CALEA), Pub. L. No. 103-414, § 103(a)(1), 108 Stat. 4279 (1994) (codified at 47 U.S.C. §§ 1001–1010). https://www.gpo.gov/fdsys/granule/STATUTE-108/STATUTE-108-Pg4279/content-detail.html; *In re Communications Assistance for Law Enforcement Act & Broadband Access & Services.*, 20 F.C.C. Rcd. 14989, ¶¶ 25, 39 (Sept. 23, 2005). https://apps.fcc.gov/edocs_public/attachmatch/FCC-05-153A1.pdf.

78. Stephanie K. Pell, "You Can't Always Get What You Want: How Will Law Enforcement Get What It Needs in a Post-CALEA, Cybersecurity-Centric Encryption Era?", *North Carolina Journal of Law and Technology* 17:4 (2016), p. 643. http://ncjolt.org/you-cant-always-get-what-you-want-how-will-law-enforcement-get-what-it-needs-in-a-post-calea-cybersecurity-centric-encryption-era.

79. See, e.g., Eliza Sweren-Becker, "This Map Shows How the Apple-FBI Fight Was About Much More Than One Phone," *American Civil Liberties Union*, March 30, 2016. https://www.aclu.org/blog/privacy-technology/internet-privacy/map-shows-how-apple-fbi-fight-was-about-much-more-one-phone; Soghoian, p. 423. http://www.jthtl.org/content/articles/V8I2/JTHTLv8i2_Soghoian.PDF.

80. Mike McConnell et al., "Why the Fear Over Ubiquitous Data Encryption Is Overblown," *The Washington Post*, July 29, 2015. https://www.washingtonpost.com/opinions/the-need-for-ubiquitous-data-encryption/2015/07/28/3d145952-324e-11e5-8353-1215475949f4_story.html; Jose Pagliery, "Ex-NSA Boss Says FBI Director Is Wrong on Encryption," *CNNMoney*, Jan. 13, 2016. http://money.cnn.com/2016/01/13/technology/nsa-michael-hayden-encryption/index.html; Jenna McLaughlin, "NSA Chief Stakes Out Pro-Encryption Position, in Contrast to FBI," *The Intercept*, Jan. 21, 2016. https://theintercept.com/2016/01/21/nsa-chief-stakes-out-pro-encryption-position-in-contrast-to-fbi.

terrorist, Rajib Karim, used a communication encryption scheme that involved first encrypting messages with custom Excel macros, saving the result in a password-protected Word document, compressing the document as an encrypted compressed file and then uploading the compressed, triply-encrypted file on an anonymous website.[81] Indeed, Karim's communications were decrypted only because investigators used a workaround to forensically retrieve the Excel spreadsheet from his computer hard disk.[82] Other, less-skilled wrongdoers likely leave evidentiary traces that are already accessible to law enforcement anyway and thus a backdoor would merely be duplicative.

All of the foregoing suggests that backdoors would be legally restrictive to law enforcement and unnecessary in the first place. Future changes to technology or better data on current law enforcement outcomes could justify a need for them in the future, but the many potential limits on their efficacy place the burden squarely on proponents to produce clear, quantifiable, objective evidence.

## ASSOCIATED POLICY RECOMMENDATIONS

### Collect quantitative evidence of need

Research should be done to quantify the need for a backdoor. Efforts such as NDCAC's Statistics Collection Tool are an important start, but that data collection could be more comprehensive and systematic. Congress could hold new hearings and consider legislative proposals for data collection, such as reporting requirements on law enforcement's collection of device data. These would be akin to the reporting requirements for wiretapping found in 18 U.S.C. § 2519, for example. Other national security experts argue that information on terrorist investigations should be declassified to provide the factual basis for any claimed need.[83]

Two caveats are appropriate with regard to this collection of statistics. First, to avoid the possibility that the government will engage in cherry-picking to serve its own interests, any data collection ought to be done objectively and subject to peer review. Second, data supporting the potential value of a backdoor will not in itself justify one; rather, that data would feed into the cost–benefit calculus of tradeoffs, which policymakers must evaluate.

As one former prosecutor wrote: "It will take more than a sampling of case anecdotes to make the case" for a backdoor.[84] Statistics on device investigative work would reveal the true extent to which encryption poses a real problem, and perhaps more importantly, they could reveal other soft spots where investigations could be improved with technological training or education. Better empirical evidence of the need is essential to advance the policy debate over encryption.

### Increase resources and training for law enforcement

Law enforcement investigators often cannot take advantage of the wealth of information offered by the "golden age of surveillance," because they lack the resources to maximize its potential and in particular, to use that information quickly enough to match the pace of the digital world.[85] Increasing resources and training would help law enforcement do its job more effectively and provide sounder evidence of whether a backdoor is still necessary once law enforcement has exhausted all of its other options.

Government-sponsored hacking or exploitation of vulnerabilities, for example, ought to be brought within a systematic legislative framework, extending and formalizing the executive branch's current Vulnerabilities Equities Process for reviewing security vulnerabilities that the government may want to exploit.[86] Formalization would help streamline the process and make it available to state and local investigators,[87] and it would also allow critical stakeholders to weigh in on the process.[88]

Additionally, government investigators ought to receive training to gain a "deep technical understanding of modern telecommunications technology and also, because all phones are computers, deep expertise in computer science."[89] Important points will likely include retrieval and use of

81. Robert Graham, "How Terrorists Use Encryption," *CTC Sentinel*, June 2016, p. 23. https://ctc.usma.edu/how-terrorists-use-encryption.

82. Ibid.

83. Jaffer and Rosenthal, p. 305. https://scholarship.law.edu/jlt/vol24/iss2/3.

84. Cordero. https://lawfareblog.com/weighing-encryption-and-going-dark-debate.

85. Marshall Erwin, "The FBI's Problem Isn't 'Going Dark.' Its Problem is Going Slowly," *Just Security*, July 16, 2015. https://www.justsecurity.org/24695/fbis-problem-going-dark-slow.

86. "Vulnerabilities Equities Policy and Process for the United States Government," The White House, Nov. 15, 2017, pp. 7–8. https://www.whitehouse.gov/sites/whitehouse.gov/files/images/External%20-%20Unclassified%20VEP%20Charter%20FINAL.PDF; Lily Hay Newman, "Feds Explain Their Software Bug Stash—But Don't Erase Concerns," *Wired*, Nov. 15, 2017. https://www.wired.com/story/vulnerability-equity-process-charter-transparency-concerns.

87. Michelle Richardson and Mike Godwin, "It's Time to Pass Legislation Governing a Key Part of the Government's Hacking Policy," *Just Security*, Oct. 5, 2017. https://www.justsecurity.org/45636/time-pass-legislation-governing-key-part-governments-hacking-policy.

88. The recent change to the criminal procedure rules, which expand the government's ability to conduct hacking under warrant garnered much criticism. Fed. R. Crim. P. 41(b)(6). See, e.g., Jadzia Butler, "U.S. Supreme Court Endorses Government Hacking," *Center for Democracy & Technology*, May 6, 2016. https://cdt.org/blog/u-s-supreme-court-endorses-government-hacking; and Jennifer Stisa Granick, "Challenging Government Hacking: What's at Stake," *American Civil Liberties Union*, Nov. 2, 2017. https://www.aclu.org/blog/privacy-technology/internet-privacy/challenging-government-hacking-whats-stake.

89. Testimony of Susan Landau, Professor of Cybersecurity Policy, House Committee on the Judiciary, "The Encryption Tightrope: Balancing Americans' Security and Privacy," 114th Congress (GPO, 2016), p. 105 (spoken error omitted). https://judiciary.house.gov/wp-content/uploads/2016/02/114-78_98899.pdf.

metadata, and also in-the-field knowledge of contemporary devices, such as the 48-hour window for biometric unlocking of some smartphones.[90] Partnerships between federal and local law enforcement, such as NDCAC, will be a key part of this learning.

## QUESTION TWO: IS THERE A PASSABLE TECHNICAL SOLUTION?

Even a strong cost–benefit showing in favor of an encryption backdoor will mean little if an actual technical solution that adequately protects public security and individual liberty does not exist.

As noted above, the current encryption debate is often couched in absolutes, with proponents of backdoors claiming that a technical solution would be easy to invent, while opponents argue that a secure backdoor is a technical impossibility. Although neither side has the definitive answer as a matter of absolute correctness, a review of the evidence leans heavily toward a comprehensive technical solution being extremely hard to develop.

Law enforcement and others who advocate for a backdoor appear to believe that developing one would be simple, which is why several current legislative proposals simply mandate technology companies to create one without regard for the necessary technical mechanism.[91] Yet experience with past attempts at backdoors shows that such systems are hardly simple. Backdoors raise numerous concerns about increased cyberattack surface and attractiveness to hackers that have been well-covered by others;[92] two of these concerns are worth mention here.

First, encryption backdoors would limit progress in developing better encryption and in patching vulnerabilities as they are discovered. For example, perfect forward secrecy is a class of encryption technologies being rolled out today, which use frequently rotating encryption keys to ensure that theft of one key does not compromise future communications.[93] A backdoor system that requires messages to be encrypted with a single government-accessible key (sometimes called a "golden key" backdoor[94]) would render moot the development of that technology, thereby leaving individuals' communications more vulnerable to third-party interception. Indeed, perfect forward secrecy means that any backdoor applied to transitory communications will likely be inadequate from a technical perspective.

Second, bad actors may be able to modify and thus commandeer the backdoor system in ways that not only give them access to encrypted communications but also keep the government out. The Dual EC algorithm previously discussed was supposed to have contained a backdoor in the form of a numeric parameter called Q. That parameter had properties known only to the NSA that enabled it to guess encryption keys quickly.[95] The Q value thus acted as a sort of "golden key." However, in 2015 it was discovered that someone had used a software update to change the Q value in one program using the algorithm, which suggested that someone other than the NSA had gained the power to decrypt messages encrypted by that program.[96] In other words, encryption backdoors can be broken into not just by obtaining the government's keys, but by changing the backdoor's locks.

At the same time, some of the stronger views as to the impossibility of a technically secure backdoor may be overly simplistic. As one scholar points out, if a method of breaking a backdoor "takes 1000 years to develop, then it doesn't matter" that the backdoor is theoretically vulnerable to such a time-consuming method of breaking.[97] Furthermore, there may exist more limited-domain backdoors that overcome at least some of the technical challenges identified for all-purpose ones. For example, one criticism of "key escrow" backdoors, in which the government is given a copy of encryption keys, is that it would be difficult "to safely transport the key to the key escrow location" and "to securely store that key alongside millions—or potentially billions—of other keys."[98] However, others have proposed "device-specific" backdoors for smartphones, in which case the encryption key can be

90. Because the FBI apparently did not know of this window, it missed the opportunity to unlock the phone of a recent mass shooting attacker. See Nick Statt, "Apple Says It Immediately Contacted FBI About Unlocking Texas Shooter's iPhone," *The Verge*, Nov. 8, 2017. https://www.theverge.com/2017/11/8/16626452/apple-fbi-texas-shooter-iphone-unlock-encryption-debate.

91. See, e.g., Richard Burr and Dianne Feinstein, "Intelligence Committee Leaders Release Discussion Draft of Encryption Bill," U.S. Senate, Apr. 13, 2016. https://www.feinstein.senate.gov/public/index.cfm/2016/4/intelligence-committee-leaders-release-discussion-draft-of-encryption-legislation; "Smartphone Encryption and Public Safety," p. 32. https://www.manhattanda.org/wp-content/themes/dany/files/Report%20on%20Smartphone%20Encryption%20and%20Public%20Safety:%20An%20Update.pdf; and Cyrus Farivar, "Yet Another Bill Seeks to Weaken Encryption-by-Default on Smartphones," *Ars Technica*, Jan. 21, 2016. https://arstechnica.com/tech-policy/2016/01/yet-another-bill-seeks-to-weaken-encryption-by-default-on-smartphones.

92. See Neumann et al., pp. 2–3. http://www.csl.sri.com/users/neumann/cacm237.pdf; and "*The Ground Truth About Encryption,*" pp. 11–12. https://www.chertoffgroup.com/files/238024-282765.groundtruth.pdf.

93. Whitfield Diffie et al., "Authentication and Authenticated Key Exchanges," *Designs, Codes, and Cryptography* 2:2 (1992), p. 107. http://people.scs.carleton.ca/~paulv/papers/sts-final.pdf; Adam Langley, "Protecting Data for the Long Term with Forward Secrecy," *Google Online Security Blog*, Nov. 22, 2011. https://security.googleblog.com/2011/11/protecting-data-for-long-term-with.html.

94. "*The Ground Truth About Encryption,*" p. 5. https://www.chertoffgroup.com/files/238024-282765.groundtruth.pdf.

95. Stephen Checkoway et al., "A Systematic Analysis of the Juniper Dual EC Incident," *Proceedings of the ACM SIGSAC Conference on Computer and Communications Security*, 2016, p. 468. https://eprint.iacr.org/2016/376.pdf.

96. Matthew Green, "On the Juniper Backdoor," *A Few Thoughts on Cryptographic Engineering*, Dec. 22, 2015. https://blog.cryptographyengineering.com/2015/12/22/on-juniper-backdoor.

97. Herb Lin, "Making Progress on the Encryption Debate," *Lawfare*, Feb. 4, 2015. https://www.lawfareblog.com/making-progress-encryption-debate.

98. "*The Ground Truth About Encryption,*" p. 6. https://www.chertoffgroup.com/files/238024-282765.groundtruth.pdf.

escrowed on the physical phone itself, thus avoiding the transport and storage issues entirely.[99] This does not mean that a device-stored key escrow backdoor is a technically sound solution (among other things, the backdoor should not be usable by phone thieves), but it is to suggest that it may be too early to say that backdoors are a technical impossibility.

As with the initial cost-benefit question, in the end, arguments against the existence of a technical backdoor solution are likely correct, but they are not necessarily conclusive in view of new ideas for backdoors of more limited scope.

## ASSOCIATED POLICY RECOMMENDATIONS

### Conduct adversarial testing

To answer the question of whether a technical solution exists, our recommended approach is actual research and experimentation. In particular, we propose an "adversarial testing" process, in which one or more technical backdoor solutions are proposed and opened up to other researchers to show flaws, gaps or insecurities in those solutions.

Several experts have proposed experimentation and testing to prove one way or another whether there is a workable technical backdoor solution. One believes that the proponents of a backdoor should "propose a specific NOBUS mechanism" (using an acronym for "nobody but us" that refers to a backdoor) and put it up for technical scrutiny.[100] Another proposes a stress test. Or put more simply, the idea that a backdoor should be used only if "the methodology for that technology has been published publicly for more than 12 months and no efforts to subvert or defeat it have been successful."[101]

An excellent model for adversarial testing may be found in the development of the Advanced Encryption Standard, an encryption algorithm that is standardized and in use today. In the process of its creation, The National Institute of Standards and Technology sought proposals for encryption technologies from the technology community, opened up those proposals for peer review and finally selected a winning technology based upon the results.[102]

The alternatives to an open-testing process include development of the backdoor by a government commission,[103] or tasking industry to create one on its own initiative.[104] Neither is preferable. Both the creation of a backdoor and stress-testing to find flaws are processes that require creativity and ingenuity. It is unlikely that the best ideas will come either from a government-sponsored commission or from the business industry. Widespread input from academics, technologists and thinkers is the best way to ensure that all facets of the encryption backdoor question are addressed.

## QUESTION THREE: IS THERE A WORKABLE POLICY IMPLEMENTATION?

Even if a technical solution to "going dark" is found to be adequately secure and protective of important interests, the task still remains for lawmakers to turn that technical solution into national and global policy. And, the subsequent problems to be addressed are numerous, difficult and likely intractable. For purposes of illustration, this section will discuss a hypothetical backdoor applied to smartphones, but the policy problems identified here could also apply to backdoors for different technologies such as cloud data storage or communications.

For starters, policymakers will have to assess the complex and costly tradeoffs required to place the backdoor in service in a way that would guarantee its almost-universal adoption. Consumer incentives to buy devices with backdoors likely will not work,[105] so the government may have to mandate inclusion of the backdoor on smartphones. But devices already in use would not be equipped with one, which means that widespread adoption could take years. A more rapid method would be for the government to pay for new phones for everyone (akin to the digital television transition) or to render the cell phone networks incompatible with older devices. Either way, the monetary costs would be enormous,[106] and there is a real question as to whether the value of the backdoor would outweigh such costs.

Policymakers would also have to lay out the rules for when and how the backdoor could be used, in ways akin to CALEA or ECPA. Numerous recent and historical events have shown that law enforcement is wont to use surveillance capabilities

99. Jamil N. Jaffer and Daniel J. Rosenthal, "Decrypting Our Security: A Bipartisan Argument for a Rational Solution to the Encryption Challenge," *Catholic University Journal of Law and Technology* 24:2 (2016), p. 309. https://scholarship.law.edu/jlt/vol24/iss2/3; "Decrypting the Encryption Debate," pp. 50–51. https://www.nap.edu/catalog/25010/decrypting-the-encryption-debate-a-framework-for-decision-makers.

100. Lin. https://www.lawfareblog.com/making-progress-encryption-debate.

101. Paul Rosenzweig, "Testing Encryption Insecurity: A Modest Proposal," *Lawfare*, July 7, 2015. https://lawfareblog.com/testing-encryption-insecurity-modest-proposal.

102. James Nechvatal et al., "Report on the Development of the Advanced Encryption Standard (AES)," *Journal of Research of the National Institute of Standards and Technology* 106:3 (2001), p. 511. http://nvlpubs.nist.gov/nistpubs/jres/106/3/j63nec.pdf.

103. H.R. 4561, 114th Congress (2016); S. 2604, 114th Congress (2016); Jaffer and Rosenthal, pp. 305–06. https://scholarship.law.edu/jlt/vol24/iss2/3.

104. Burr and Feinstein. https://www.feinstein.senate.gov/public/index.cfm/2016/4/intelligence-committee-leaders-release-discussion-draft-of-encryption-legislation.

105. One can imagine offering the backdoor as a consumer feature, for example, to recover data from the phone if it is damaged or the password is forgotten. But advertising a backdoor as a feature is unlikely to persuade, and frequent consumer use of backdoors would introduce significantly greater complexity to the development of technical and policy solutions.

106. See Eliot Van Buskirk, "How We Bungled the Digital Television Transition," *Wired*, Feb. 20, 2009. https://www.wired.com/2009/02/how-the-governm.

for personal or political gain.[107] Detailed procedural requirements, akin to the Woods Procedures that the FBI uses prior to conducting surveillance under FISA,[108] would be especially important to prevent abuses of a backdoor that could potentially reveal highly private and personal information. Transparency interests would also require consideration: Smartphone users will want to be sure that no one is secretly using the backdoor to snoop on them, but law enforcement will likely want to be able to conduct investigations in secret.

If keys or other components of the backdoor are maintained on third-party or government computer systems, then cybersecurity and data breach notification laws would be necessary. The government has proven on several occasions that it cannot maintain security of sensitive data from hackers.[109] Indeed, the Transportation Security Administration once accidentally allowed its backdoor keys for luggage locks to be published in a photo in the Washington Post.[110] Lawmakers have struggled with data breach and cybersecurity questions in the comparatively simpler field of personal data collection,[111] and they are likely to face greater difficulties with regard to a backdoor.

The government would almost certainly want a program for ongoing white-hat testing of the backdoor to discover unexpected flaws or vulnerabilities. Numerous recent events remind us that even systems designed to be as secure as possible can fall victim to software bugs or mistakes,[112] making continuous review necessary. But that poses a dilemma: Opening up the backdoor to researchers raises the possibility that a malicious actor could pose as a researcher to gain unauthorized access to confidential aspects of the backdoor. Developing satisfactory testing policy may thus prove to be an unusually hairy problem of security clearances and background checking.

Use of a backdoor as a tool for mass surveillance is a concerning problem that must be addressed. People often leave their smartphones unattended in a variety of circumstances, such as when crossing the national border[113] or when at school.[114] For this reason, it would be economically and socially detrimental if people were faced with the possibility that their phones could be decrypted on a regular basis. Technological solutions, such as making the backdoor time-consuming or difficult to use, can help but may not be sufficient.

Issues of federalism also come into play. Several states have attempted to introduce encryption backdoor legislation already.[115] These would likely be unduly burdensome on national- or global-scale companies, so federal preemption would be appropriate and warranted.[116] But state and local law enforcement will probably be the more frequent users of any encryption backdoor and thus federal legislation will need to develop rules for information-sharing between federal and state authorities. In the past, local law enforcement's failure to understand the legal ramifications of surveillance technology have already caused otherwise airtight cases to be thrown out, rendering the technology moot.[117]

Most importantly, there would have to be a contingency plan in case the backdoor is widely breached by a third party, a risk that can be minimized but almost certainly never eliminated. National security interests would be at stake, especially in the likely case that government and military personnel use the same devices as civilians. Likely the only secure solution is to replace all smartphones with the backdoor, a costly proposition for which the government must prepare.

Globalization presents even greater policy difficulties. If backdoor keys are stored externally on third-party servers, then every nation will vie to have copies and will likely impose pressures on device manufacturers or one another to

107. Andrea Peterson, "LOVEINT: When NSA Officers Use Their Spying Power on Love Interests," *The Washington Post*, Aug. 24, 2013. https://www.washingtonpost.com/news/the-switch/wp/2013/08/24/loveint-when-nsa-officers-use-their-spying-power-on-love-interests; Ellen Nakashima, "Justice Dept. Told Court of Source's Political Influence in Request to Wiretap Ex-Trump Campaign Aide, Officials Say," *The Washington Post*, Feb. 3, 2018. https://www.washingtonpost.com/world/national-security/justice-dept-told-court-of-sources-political-bias-in-request-to-wiretap-ex-trump-campaign-aide-officials-say/2018/02/02/caecfa86-0852-11e8-8777-2a059f168dd2_story.html.

108. See, e.g., Testimony of Robert S. Mueller, III, Director, Federal Bureau of Investigation, Senate Committee on the Judiciary, "Oversight Hearing on Counterterrorism," 107th Congress (GPO, 2002), pp. 14–15 and 260-73. https://www.gpo.gov/fdsys/pkg/CHRG-107shrg86517/pdf/CHRG-107shrg86517.pdf.

109. Brendan I. Koerner, "Inside the OPM Hack, the Cyberattack That Shocked the US Government," *Wired*, Oct. 23, 2016. https://www.wired.com/2016/10/inside-cyberattack-shocked-us-government; David Perera, "Researcher: Voter Registration Data of 191 Million Exposed Online," *Politico*, Dec. 28, 2015. https://www.politico.com/story/2015/12/voter-registration-data-exposed-217172.

110. Nicholas Weaver, "A Tale of Three Backdoors," *Lawfare*, Aug. 27, 2015. https://www.lawfareblog.com/tale-three-backdoors.

111. Rachel German, What Are the Chances for a Federal Breach Notification Law?", *Center for Identity, University of Texas at Austin*, April 14, 2015. https://identity.utexas.edu/id-experts-blog/what-are-the-chances-for-a-federal-breach-notification-law.

112. See, e.g., Thomas Fox-Brewster, "The Feds Can Now (Probably) Unlock Every iPhone Model in Existence," Forbes, Feb. 26, 2018. https://www.forbes.com/sites/thomasbrewster/2018/02/26/government-can-access-any-apple-iphone-cellebrite.

113. Morgan Chalfant, "Homeland Security Sued over Warrantless Phone, Laptop Searches at Border," *The Hill*, Sept. 13, 2017. http://thehill.com/policy/cybersecurity/350449-dhs-sued-over-warrantless-electronic-device-searches-at-border.

114. Amy E. Feldman, "When Does a Public School Have the Right to Search Its Students?", *National Constitution Center*, May 31, 2013. https://constitutioncenter.org/blog/when-does-a-public-school-have-the-right-to-search-its-students.

115. Farivar. https://arstechnica.com/tech-policy/2016/01/yet-another-bill-seeks-to-weaken-encryption-by-default-on-smartphones.

116. H.R. 4528, Ensuring National Constitutional Rights for Your Private Telecommunications Act of 2016, 114th Congress (2016).

117. Robert Patrick, "Controversial Secret Phone Tracker Figured in Dropped St. Louis Case," *St. Louis Post-Dispatch*, April 19, 2015. http://www.stltoday.com/news/local/crime-and-courts/controversial-secret-phone-tracker-figured-in-dropped-st-louis-case/article_fbb82630-aa7f-5200-b221-a7f90252b2d0.html.

gain access.[118] And at the time law enforcement seeks to use a backdoor with the keys held in another country, mutual legal assistance treaties would come into play.[119] Requests under these treaties can be slow and complicated,[120] which could frustrate the value of any backdoor. Finally, the presence of one within the United States could have economic repercussions for global trade, as foreign businesses that want to avoid communicating with backdoor-vulnerable systems might stop manufacturing for the U.S. market or doing business with U.S. companies altogether.[121]

If any backdoor system is adopted, it must not only be secure as a technological matter. It must also be implemented with policy that solves the many problems discussed above, as well as others that will likely arise. This is a serious challenge that unfortunately does not appear to be addressed sufficiently in the current debate thus far. When it comes to putting a backdoor into practice, the policy difficulties will almost certainly exceed even the technical ones.

## ASSOCIATED POLICY RECOMMENDATIONS

### Conduct scenario planning

To address the question of what laws and policies must be in place to implement a technical backdoor, we recommend systematic thinking, and in particular, scenario planning as to ways that the backdoor could fail or otherwise be misused in practice. Scenario planning is a common practice that largely originates in the field of military strategy and came into common use after World War II.[122] Now extended to business settings as well, the practice involves statistical modeling or other analysis to develop reasonably detailed scenarios that can be planned for in advance.[123]

Done correctly and comprehensively, scenario planning could highlight the many potentially difficult situations that an encryption backdoor could face, including a government data breach, law enforcement misuse of the backdoor or malicious hacking efforts. Detailing these possible scenarios could help to put into focus the many policy tradeoffs that lawmakers would have to make in order to implement even a theoretically secure backdoor. This would move the debate beyond its current single hypothetical proposition.

## CONCLUSION

As with many things, when it comes to encryption, reality is complicated. And when reality is complicated, there is a tendency to fall back on easy hypotheticals: the terrorist's cell phone with all the secrets encrypted or the government's golden decryption key too easily stolen by hackers. However, policymakers should avoid that trap, embrace the complexity of reality, and tackle *real* questions about how to deal with "going dark" in practice and what implementation of an encryption backdoor would look like in reality.

The time to answer these questions is now. The worst-case scenario for the encryption debate is a terrorist attack or other emergency threat that pushes Congress to enact an ill-conceived encryption backdoor mandate that is not justified either by actual law enforcement needs or by technological study. To avoid such a scenario requires laying the groundwork for research into the relative costs and benefits, workable technical solutions and policy implementation. Doing so requires a deliberate attempt to move past the current thought-experiment debates that have so far stymied pragmatic progress.


### ABOUT THE AUTHORS

**Charles Duan** is a senior fellow and associate director of tech and innovation policy at the R Street Institute, where he focuses his research on intellectual property issues. Before joining R Street in January 2018, Charles was the director of the patent reform project at Public Knowledge, where he handled all aspects of patent policy ranging from outreach on the Hill to writing white papers and filing amicus briefs. Prior to this, he was a research associate to Professor Paul Ohm on an NSF-funded project that investigated the policy implications of newly proposed Internet architectures. He also worked as a patent attorney at Knobbe Martens.

**Zach Graves** is director of technology and innovation policy for the R Street Institute, where he manages development efforts for the tech program, oversees its scholars and coordinates work across a variety of issue areas. Zach joined R Street in April 2013, having previously worked at the Cato Institute and the America's Future Foundation. He is also a fellow at the Internet Law and Policy Foundry and a visiting fellow at the National Security Institute at George Mason University's Antonin Scalia Law School.

**Arthur Rizer** is director of justice and national security policy for the R Street Institute, where he heads institute programs dealing with a variety of issues related to intelligence, national security, crime and policing. In this capacity, he produces original research,


118. Already China has pressured Apple into making encryption keys more easily available to the government. See, e.g., Thuy Ong, "Apple Will Store Some iCloud Encryption Keys in China, Raising Security Concerns," *The Verge*, Feb. 26, 2018. https://www.theverge.com/2018/2/26/17052802/apple-icloud-encryption-keys-storage-china.

119. Arthur Rizer and Anne Hobson, "Cross-Border Data Requests: Evaluating Reforms to Improve Law Enforcement Access," *R Street Policy Study* No. 120, November 2017. http://www.rstreet.org/policy-study/cross-border-data-requests-evaluating-reforms-to-improve-law-enforcement-access.

120. Ibid., p. 4.

121.For comparison, national security concerns about malicious computer systems led Congress to ban use of Russian software on government computers and led AT&T to drop a plan to sell certain Chinese phone handsets. See Dustin Volz, "Trump Signs into Law U.S. Government Ban on Kaspersky Lab Software," *Reuters*, Dec. 12, 2017. https://www.reuters.com/article/us-usa-cyber-kaspersky/trump-signs-into-law-u-s-government-ban-on-kaspersky-lab-software-idUSKBN1E62V4; and Paul Mozur, "AT&T Drops Huawei's New Smartphone Amid Security Worries," *The New York Times*, Jan. 10, 2018. https://www.nytimes.com/2018/01/09/business/att-huawei-mate-smartphone.html.

122. Ron Bradfield et al., "The Origins and Evolution of Scenario Techniques in Long Range Business Planning," Futures 37:8 (2005), pp. 797–98. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.322.703&rep=rep1&type=pdf.

123. Paul J.H. Schoemaker, "Scenario Planning: A Tool for Strategic Thinking," Sloan Management Review 36:2 (1995), pp. 27–30. http://www.ftms.edu.my/images/Document/MOD001074%20-%20Strategic%20Management%20Analysis/WK4_SR_MOD001074_Schoemaker_1995.pdf.

writes for the popular press and educates policymakers on national security and criminal justice issues. Arthur joined R Street in August 2016, having previously served as associate professor of law at West Virginia University's College of Law and visiting professor of law at Georgetown University Law Center.

**Mike Godwin** is a distinguished senior fellow at the R Street Institute, where he focuses on the areas of patent and copyright reform, surveillance reform, technology policy, freedom of expression and global internet policy. Before joining the R Street Institute in 2015, he served as a senior policy advisor at Internews, advising the organization's public-policy partners in developing and transitional democracies, as part of the Global Internet Policy Project. Prior to his return to Washington, he served as general counsel for the California-based Wikimedia Foundation, which operates Wikipedia and other collaborative projects. At the foundation, he created and directed anti-censorship, privacy, trademark and copyright strategies, and policies including Wikimedia's responses to the SOPA and PIPA initiatives. Godwin received his undergraduate and law degrees at the University of Texas at Austin where, while a law student, he served as a reporter and later editor-in-chief of *The Daily Texan*. Upon graduation, Godwin began his legal career as the first staff counsel for the Electronic Frontier Foundation, which he advised on a range of legal issues centered on freedom of expression and privacy rights during the accelerated growth of Internet access in the United States. His continuing career as an Internet-law thought leader has included a policy fellowship at the Center for Democracy and Technology and a research fellowship at Yale Law School. He has been a contributing editor at *Reason* magazine since 1994 and is the originator of the widely cited "Godwin's Law of Nazi Analogies," which in 2012 was added to the *Oxford English Dictionary*.

LAWFARE

ENCRYPTION

# A New Framework for the Encryption Debate

By **Charles Duan** Monday, April 9, 2018, 1:12 PM

The New York Times reported on March 24 that the FBI and Justice Department are again pushing for extraordinary access to encrypted data. This will certainly set off yet another round of the long-standing debate over encryption.

This debate has made little progress. Those in favor of giving law enforcement extraordinary, or "backdoor," access to encrypted data argue that there is no way to protect public safety in a world of unbreakable encryption. And those against say that any form of extraordinary access will create mass vulnerabilities and leave basic internet infrastructure insecure. The recent report of the National Academies on encryption describes this debate as "very polarized."

Given this polarized posturing, it may seem like the debate is at an impasse. Yet several commentators, including the authors of the National Academies report and contributors to *Lawfare*, have looked for new ways to advance the debate. In a recent paper, my colleagues Arthur Rizer, Zach Graves, Mike Godwin and I synthesize these ideas and others to propose a way forward on encryption policy.

We propose a three-part test for policymakers, with each part tied to specific action items that may be addressed by advocates on either side of the debate. The test is designed to advance the discussion of whether extraordinary access can be justified. First, we ask whether there is empirical evidence for the need for extraordinary access. Second, we ask whether an acceptable technology already exists for such access. Last, we ask whether adequate policy and legal frameworks can be developed to put that technology safely into practice.

In light of these questions, the New York Times report is both promising and concerning. It notes that the Justice Department has been working with computer scientists on developing a technological system limited to encrypted smartphones, in line with the second question we ask. Yet any technology that might result from this reportedly "quiet" collaboration is unlikely to satisfy the test we propose.

First, notional systems for extraordinary access to encrypted data will be sensitive and require thorough evaluation to find flaws. If research is conducted behind closed doors, the Justice Department is diminishing its ability to benefit from out of the box thinking, criticism and troubleshooting. For example, the Spectre and Meltdown vulnerabilities that used processor timing to reveal passwords were present in Intel processors for decades and only discovered recently because of some truly creative testing. When it comes to extraordinary access technology, an open peer review and testing process (akin to the National Institute for Standards and Technology contest for developing the Advanced Encryption Standard) is more likely to ensure that the best minds can identify any unexpected flaws that would leave vulnerable a seemingly secure extraordinary-access system. Although one could envision an extraordinary-access system where the technology is kept secret, the general consensus among cryptographers is that the better path forward is an open and well-tested system with only the government's internal keys kept secret; secret algorithms are "something likely to make a system prone to catastrophic collapse."

Second, research into extraordinary-access systems may ultimately be wasteful if it turns out that, in view of other surveillance and investigation methods, law enforcement does not actually need extraordinary access to encrypted data. Indeed, recent events suggest only that the case for extraordinary access is now weaker: the recent report that the Justice Department slow-walked efforts to unlock San Bernardino shooter's phone, as Susan Landau has explained on *Lawfare*, "casts doubt on the argument" in favor of extraordinary access.

Finally, in addition to calling for an open process for researching technology, we also call for an open discussion of the policy framework that will implement that technology. Designed correctly, an extraordinary-access system will include not just chips on phones or specialized encryption algorithms, but also laws to compel or encourage adoption of the system, to control how law enforcement uses its power to read encrypted messages and to deal with the fallout if something goes wrong. The Trump administration is apparently engaging in internal dialogue on legislation, but it is an open question whether that dialogue will deal with some of these policy questions, and there is as of yet no indication that the Justice Department or the administration is convening policy experts along with the technologists.

Here are just a few policy implementation questions: How will the extraordinary-access system includes accountability and auditing to ensure that law enforcement doesn't misuse the backdoor to spy on friends or enemies? How will local law enforcement work with federal agencies to obtain access? How will the security of the backdoor be tested on an ongoing basis to ensure that software implementations don't have bugs or errors? What happens if a serious flaw is found in the implementation—is there a process for recalling or patching every device? How will law enforcement deal with cross-border investigative requests, while resisting pressures from foreign governments to open up extraordinary access beyond what the United States may deem acceptable? Our paper identifies further policy questions like these; the National Academies report advances even more.

Answering questions like these will be at least as important, and likely more difficult, than devising the technology itself. Indeed, solving these problems will probably overwhelm the project. But that is no excuse for not trying. It is the responsibility of those calling for extraordinary access to have in hand not only a viable technology but also the policy framework accompanying that technology.

**Topics: Encryption**

---

Charles Duan is a senior fellow and associate director of tech & innovation policy at the R Street Institute, where he focuses his research on intellectual property issues.

OPINION

# New FTC Leadership Should Focus on Results, Not Headlines

BY **TOM STRUBLE**
May 18, 2018

After nearly three years of top-level vacancies, our nation's chief competition and consumer protection agency, the Federal Trade Commission, is finally back to full strength. Accordingly, many are now looking at the FTC with fresh optimism, hoping its new leadership can help tackle the most challenging issues facing consumers and competitors today.

I share this hope, but want to urge a note of caution: Good headlines don't always yield good results.

Much of the important work the FTC does tends to fly below the radar. For example, the FTC recently convinced tech giants Uber and Qualcomm to improve their privacy and patent-licensing practices, respectively. Additionally, outside the Part 3 enforcement process, the FTC recently tackled the tricky topic of informational injuries, seeking to better understand how Section 5's consumer-protection framework can account for non-financial privacy harms — like personal embarrassment, general feelings of creepiness or even potential interference with the electoral process. From safer ride-hailing services and cheaper smartphones to a framework better equipped to tackle the difficult privacy issues of the 21st century, these moves will yield meaningful and lasting benefits for millions of American consumers.

But reports of these efforts rarely stick in the headlines for more than a day or two — if they make it there at all — and that's a shame. Instead, Americans see vast amounts of ink spilled over high-profile investigations into Facebook and Equifax's recent privacy mishaps, the ongoing antitrust challenge to AT&T's acquisition of Time Warner, and what regulators in the European Union are set to impose later this month with their General Data Protection Regulation.

Chairman Joseph Simons and Commissioners Noah Philips, Christine Wilson, Rohit Chopra and Rebecca Slaughter are all surely aware of these headlines, and there will be much pressure to respond to this vocal outrage by doing something. But the FTC's mandate isn't to "do something" — it is to promote the welfare of consumers. It's through this consumer-welfare lens that Section 5's competition and consumer-protection standards have developed over time to accommodate new technologies, business models and economic learning — all of which have proven to be a tremendous boon to American consumers and the economy writ large. This body of work should not be cast aside lightly.

To see what happens when competition agencies go for headlines rather than real improvements, consider European Union Competition Commissioner Margrethe Vestager, who has been making headline after headline in her aggressive pursuit of major tech companies. Recently, she issued fines of $122 million to Facebook, $1.2 billion to Qualcomm and $2.7 billion to Google. These are big numbers, but they aren't necessarily real results. For one thing, Qualcomm and Google are appealing the latter two fines, so this money may never make its way to European coffers. More importantly, though, it's unclear whether European consumers are any better off today because of such efforts. Arguably, aggressive fines and the sweeping new GDPR rules will

actually make Europe even less friendly to investment and innovation, further widening the gap between their technology ecosystem and ours.



If the FTC is going to make good on its core consumer commitment, it can start by looking under the hood at its own procedures. William Kovacic, a former FTC chairman, recently made this point to The Washington Post: "As a country, do we want to do this on the cheap, or do we want to do this the right way? And in a sense, we've been trying to do it on the cheap."

Indeed, academics and civil society groups have long decried FTC process failures that have undercut the agency's dual mission of protecting consumers and competition. Internal-process reforms will likely never make front-page news, but they can have a tremendous impact on consumer welfare if they are done right. Such reforms may include reinvigorating the FTC's Part 3 adjudicatory process — something Simons spoke highly of while directing the FTC's Competition Bureau in the early 2000s — or finally undertaking a consumer-protection rulemaking under Section 18.

Ultimately, what matters most is not the number of complaints or the size of fines. What matters are the actual effects that FTC guidance and enforcement (or lack thereof) have on consumer welfare. Those results aren't easy to come by; they take hard work, due diligence and a fair amount of patience. These efforts don't make for catchy headlines, but they do yield great outcomes for consumers. In these chaotic and

headline-driven times, the new FTC leadership would do well to keep this in mind.

*Tom Struble is technology policy manager at the R Street Institute, a free-market think tank based in Washington, D.C.*

Morning Consult welcomes op-ed submissions on policy, politics and business strategy in our coverage areas. Updated submission guidelines can be found here.

TECH

**Before the Federal Trade Commission**

| | |
|---|---|
| In re:<br>Competition and Consumer Protection in the 21st Century Hearings<br><br>Topic 9: The consumer welfare implications associated with the use of algorithmic decision tools, artificial intelligence and predictive analytics | Project No. P181201<br>Docket No. FTC-2018-0056 |

**Comments of the R Street Institute**

In response to the Federal Trade Commission's request for comments dated June 20, 2018, the R Street Institute respectfully submits the following comments. Submitted in advance of the hearings planned to be held, these are intended to identify topics for those hearings, and will likely be supplemented by more detailed analysis afterward.

This comment is one of several that R Street is submitting, pursuant to the Commission's request of a separate comment per topic. This comment relates to Topic 9 on the consumer welfare implications associated with the use of algorithmic decision tools, artificial intelligence (AI), and predictive analytics.

Continued progress in AI and algorithmic decision making holds great promise for consumer benefit and for American national security. The Commission has already begun to examine the implications of AI for competition policy, particularly within the realm of financial technology.[1] However, AI and algorithms play a role in our economy far beyond the financial sector and the Commission is wise to have included a broad discussion in the upcoming hearings.

In addition to the issues already identified in Topic 9, we therefore encourage the Commission also to consider the following topics.

**Dynamics of International Regulatory Competition Around AI.** While the Commission has traditionally focused on domestic competition, in an increasingly globalized world, international regulatory actions by the Chinese and European Union (EU) governments, in particular, will be very relevant for the behavior of large multinational firms and startups alike in the United States. For example, the recently enacted General Data Protection Regulation in the EU contained an explainability requirement for algorithms used to make automated decisions about EU consumers.[2] The Commission should pay close attention to the effect of this and

[1] See, e.g., "FinTech Forum: Artificial Intelligence and Blockchain," Federal Trade Commission, March 9, 2017. https://www.ftc.gov/news-events/events-calendar/2017/03/fintech-forum-blockchain-artificial-intelligence.
[2] See, e.g., Bryce Goodman and Seth Flaxman, "European Union regulations on algorithmic decision-making and a 'right to explanation'" *AI Magazine* 38:3 (2017). https://arxiv.org/abs/1606.08813; and Lilian Edwards and Michael Veale, " Slave to the Algorithm? Why a 'Right to an Explanation' Is Probably Not the Remedy You Are Looking For,"

similar provisions, both in the response of multi-national firms (do they chose to offer different services or different pricing models in the EU vs the US?) and in the rate of technology startup formation (do new startups choose to form or migrate to geographic regions with less restrictive AI regulations?).

The Commission should learn from these results both in terms of the regulatory proposals that should be adopted or avoided here in the United States, but also as a case study for the larger phenomenon of global innovation arbitrage.[3] Just as important as having the "correct" regulatory guidelines is an awareness of the relative strengths and weaknesses of our regulatory regime and the way they affect where innovation arises and migrates.

**Changes in Industrial Organization Resulting from AI.** As with any new general purpose technology, advances in AI are already beginning to shape the structure of new firms. Leading economists have recently begun to study this issue, but much more analysis is warranted.[4] How large are the pro-competitive effects of layering AI tools on top of distributed computing platforms? Are the returns-to-scale from data muted by the increasing importance of creative algorithmic design? Why do we not have more developed markets for data sharing? The Commission would be wise to engage deeply in this emerging conversation.

**Reducing Entry Barriers to AI Development.** Also of interest to the Commission was "whether restrictions on the use of computer and machine learning and data analytics affect innovation or consumer rights and opportunities in existing or future markets, or in the development of new business models." As a closely related question, we would also recommend examining the ways in which U.S. public policy may have inadvertently created entry barriers for the development and application of AI across the economy. Restrictions on the supply of data scientists and on the supply of publicly accessible data, for instance, may have artificially bolstered the market position of leading tech firms. The Commission would be well-positioned to study this question and connect its larger implications for competition policy.

**Competition in Datasets for AI research.** Of particular interest to the Commission may be the lack of competition that results from insufficient competitive access to data. This should be thought of primarily along two dimensions: 1) Do the existing set of legal protections around proprietary data access need to be changed? This could take the form of intellectual property review, but also through interoperability requirements. 2) Are there ways we can make existing government databases available to the public to offset incumbency advantages?

*Duke Law and Technology Review* 18 (Dec. 6, 2017). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2972855.

[3] Adam Thierer, "Innovation Arbitrage, Technological Civil Disobedience & Spontaneous Deregulation," *Technology Liberation Front,* Dec. 5, 2016. https://techliberation.com/2016/12/05/innovation-arbitrage-technological-civil-disobedience-spontaneous-deregulation.

[4] See, e.g., Hal Varian, "Artificial Intelligence, Economics, and Industrial Organization," *The Economics of Artificial Intelligence: An Agenda* (University of Chicago Press, Forthcoming). http://www.nber.org/chapters/c14017.pdf.

*  *  *

R Street thanks the Federal Trade Commission for the opportunity to submit these comments, and recommends that the Commission pursue the above-identified areas in its ongoing work on promoting competition and innovation.

Respectfully submitted,

***/s/***

Caleb Watney
*Tech Policy Fellow*

R Street Institute
1212 New York Ave, NW
Suite 900
Washington, DC  20005
cwatney@rstreet.org

August 13, 2018

**Before the Federal Trade Commission**

| | |
|---|---|
| In re:<br>Competition and Consumer Protection in the 21st Century hearings<br><br>Topic 1: The state of antitrust and consumer protection law and enforcement, and their development, since the Pitofsky hearings. | Project No. P181201<br>Docket No. FTC-2018-0048 |

**Comments of the R Street Institute**

In response to the Federal Trade Commission's request for comments dated June 20, 2018, the R Street Institute respectfully submits the following comments. Submitted in advance of the hearings planned to be held, these are intended to identify topics for those hearings, and will likely be supplemented by more detailed analysis afterward.

This comment is one of several that R Street is submitting, pursuant to the Commission's request of a separate comment per topic. This comment relates to Topic 1 on the state of antitrust and consumer protection law and enforcement, and their development, since the Pitofsky hearings.

Over twenty years ago, FTC Chairman Robert Pitofsky convened a series of public hearings "to determine whether changing economic factors, such as the development of a global economy and the growth of high-tech industries, require adjustments in current antitrust and consumer protection enforcement."[1] In the time since then, the economy has become increasingly global and dominated by high-tech industries, but these are differences in degree rather than kind. The consumer welfare standard is still the best framework for antitrust and consumer protection law, and the Commission should continue advocating for it both at home and abroad.

However, recent changes do warrant an introspective look into the Commission's investigation, enforcement and remedial processes.[2] Procedural irregularities were partially to blame for the Commission's recent loss in the *LabMD* case and similar process failures could sabotage the Commission's attempts to protect consumers in the future. With the Commission back to full

[1] Federal Trade Commission, "FTC Announces Hearings on Antitrust and Consumer Protection Laws in Global, High-Tech Economy," July 19, 1995. https://goo.gl/2G6bqL.

[2] Tom Struble, "Reforming the Federal Trade Commission Through Better Process," *R Street Policy Study* No. 122, December 2017. https://goo.gl/tEtBMN.

strength, now is a great time to consider potential reforms.[3] In the upcoming hearings, we therefore encourage the Commission to consider at least the following topics.

**Institutional Expertise and Independence.** The Commission's work is so valuable because of its institutional expertise and independence. However, both have come under assault recently. Some discount the Commission's expertise, arguing that it lacks the "specialized expertise" needed to regulate certain high-tech industries.[4] Others question its independence, saying it lacks true autonomy and acts at the behest of the administration.[5] These criticisms are poorly founded, but even the mere perception of impropriety can seriously undercut the Commission's work, both at home and abroad. Thus, as American policymakers and their foreign counterparts consider potential changes to competition and consumer protection law, the Commission should make every effort to bolster and preserve its institutional expertise and independence.

Holding public hearings will certainly help, but further steps may also be warranted. For example, moving the Office of Technology Research and Investigation out of the Bureau of Consumer Protection and into a new Bureau of Technology may help bolster the Commission's technical expertise. Nothing, however, justifies throwing out the playbook and starting anew. The Commission's singular focus on consumer welfare is what makes it the best competition and consumer protection agency in the world.[6] The increasing complexity of the modern economy is not a reason to change course. Rather, it is an opportunity for the Commission to reestablish its global leadership by developing and applying sound economic reasoning to the technical challenges that face consumers today.[7]

**Development of Legal Standards.** Administering and enforcing the broad legal standards in Section 5 requires the Commission to continually adapt to changes in industry and consumer behavior. The need for adaptation and evolution of legal standards is particularly vital for industries undergoing rapid change, as existing precedent — or, indeed, the lack thereof — can quickly come to stifle industry growth and harm consumers.[8] The Commission's overreliance on consent decrees is evidence of that. Not only do such consent decrees often fail to curb bad behavior, as seen recently with Facebook, but even worse, they sometimes punish a firm

---

[3] See, e.g., Tom Struble, "Senate Finally Poised to Restore FTC to Full Strength," *R Street Institute Blog*, Oct. 19, 2017. https://goo.gl/TQ5qrE.

[4] See, e.g., Terrell McSweeny, "The FCC Plans to Kill the Open Internet; Don't Count on the FTC to Save It," *Quartz*, Dec. 5, 2017. https://goo.gl/eg4N63.

[5] See, e.g., Andrew Orlowski, "Google had Obama's Ear During Antitrust Probe," *The Register*, Aug. 18, 2016. https://goo.gl/PtYEjd.

[6] See, e.g., Tom Struble, "New FTC Leadership Should Focus on Results, Not Headlines," *Morning Consult*, May 18, 2018. https://goo.gl/tM63Cp.

[7] See, e.g., Tom Struble, "A Positive Agenda for the New FTC," *Morning Consult*, Feb. 14, 2018. https://goo.gl/kmkwXb.

[8] See, e.g., "Reforming the Federal Trade Commission Through Better Process," p. 3. https://goo.gl/tEtBMN.

effectively to death. For example, consent decrees with Toys "R" Us and Sears were subsequently modified to loosen some of their original restrictions.[9] However, that relief came too late for the former[10] and likely too late for the latter, as well.[11]

Can this situation be improved somehow? For example, would greater focus on litigation in industries undergoing rapid evolution reduce these types of incidents, where behavioral remedies extracted via consent decrees deny firms the ability to innovate and compete in new ways? Would adjudicating more cases promote development of legal standards in areas like privacy and data security? Can the Commission reform its investigatory processes to encourage more litigation? Would allowing firms to challenge the scope of an initial civil investigatory demand under seal, without immediately making the investigation public to consumers and investors, encourage more litigation and less out-of-court settlement? Would reorganizing the Commission's internal structure to separate the investigation and enforcement processes, as some have proposed,[12] further or hinder the development of legal standards?

**Future of Part 3 Administrative Litigation.** When done well, administrative litigation not only drives evolution of the law and the development of legal principles,[13] but also provides a venue for dispute resolution that is faster and cheaper than general Article III courts. However, as Commissioner Ohlhausen recently acknowledged, there is some disagreement as to whether the Commission's Part 3 administrative litigation functions well.[14] Some may still insist that Part 3 is a "rigged system" or "kangaroo court" because the Commission exercises both quasi-executive and quasi-judicial functions in administering Section 5, but those claims are difficult to square with the data.[15] Nevertheless, there are still changes that could potentially improve both the appearance and substantive outcomes of its Part 3 administrative litigation.

For example, there is some question as to whether the Commission has enough Administrative Law Judges. In 1980, Chairman Michael Pertschuk boasted of "a corps of Administrative Law

---

[9] See, e.g., Federal Trade Commission, "Order Reopening and Modifying Order," In the Matter of Toys "R" Us Inc., Docket No. 9278, Apr. 11, 2014. https://goo.gl/nmDKqJ; Federal Trade Commission, "Order Reopening and Modifying Order," In the Matter of Sears Holdings Management Corp., Docket No. C-4264, Feb. 27, 2018. https://goo.gl/wqtW7L.

[10] See, e.g., Michael Cappetta, "Game Over as Bankrupt Toys R Us Files for Liquidation," *NBC News*, March 15, 2018. https://goo.gl/MdD6Zx.

[11] See, e.g., Lauren Coleman-Lochner and Katherine Doherty, "Sears Buoyed by Plan that Analyst Sees as Bankruptcy Hint," *Bloomberg*, May 14, 2018. https://goo.gl/gAtJQW.

[12] See, e.g., Terry Calvani and Angela M. Diveley, "The FTC at 100: A Modest Proposal for Change," *George Mason Law Review* 21:5 (2014), pp. 1183–88. https://goo.gl/YsHgst.

[13] Maureen K. Ohlhausen, "Administrative Litigation at the FTC: Effective Tool for Developing the Law or Rubber Stamp?" *Journal of Competition Law and Economics* 12:4 (2016), pp. 623–59. https://goo.gl/LbJ8yc.

[14] Ibid.

[15] Ibid., p. 657.

Judges who are competent, impartial, and independent"[16] but today the Commission's Chief Administrative Law Judge, D. Michael Chappell, is its only judge. The Commission now also adjudicates only a handful of cases each year, which leads some to wonder whether it is even worth maintaining the Part 3 process.[17] Should the Commission abandon Part 3 entirely, reinvigorate the process, or maintain its current level of minor use? How does the Department of Justice factor into it? Would eliminating Part 3 facilitate coordination between the Commission and Department of Justice in the development of competition law? Could the Justice Department be allowed to participate in Part 3 proceedings, as amicus curiae or otherwise? What impact would that have on the Commission's institutional independence?

* * *

R Street thanks the Federal Trade Commission for the opportunity to submit these comments, and recommends that the Commission pursue the above-identified areas in its ongoing work on promoting competition and innovation.

Respectfully submitted,

***/s/***

Tom Struble
*Tech Policy Manager*

R Street Institute
1212 New York Ave, NW
Suite 900
Washington, DC 20005
tstruble@rstreet.org

August 14, 2018

[16] Federal Trade Commission, "Testimony of Michael Pertschuk, Chairman, Federal Trade Commission, Before the Senate Consumer Subcommittee, Committee on Commerce, Science and Transportation," Sept. 4, 1980, p. 2. https://goo.gl/8HTPB3.

[17] See, e.g., David Balto, "McWane: Why Have an Administrative Law Judge?" *Truth on the Market*, Jan. 17, 2014. https://goo.gl/eSaQxb.

**Before the Federal Trade Commission**

| | |
|---|---|
| In re:<br>Competition and Consumer Protection in the 21st Century Hearings<br><br>Topic 5: The Commission's Remedial Authority to Deter Unfair and Deceptive Conduct in Privacy and Data Security Matters | Project No. P181201<br>Docket No. FTC-2018-0052 |

**Comments of the R Street Institute**

In response to the Federal Trade Commission's request for comments dated June 20, 2018, the R Street Institute respectfully submits the following comments. Submitted in advance of the hearings planned to be held, these are intended to identify topics for those hearings, and will likely be supplemented by more detailed analysis afterward.

This comment is one of several that R Street is submitting, pursuant to the Commission's request of a separate comment per topic. This comment relates to Topic 5 on the Commission's remedial authority to deter unfair and deceptive conduct in privacy and data security matters.

Privacy and data security are increasingly vital to the American public.[1] The Commission has done an admirable job in these areas by offering recommendations for business and policymakers,[2] as well as by pursuing legal actions where appropriate,[3] but not all these efforts have been successful. Indeed, the recent setback in its case against LabMD suggests that significant changes may need to be made in how the Commission pursues privacy and data security cases going forward.[4]

In the upcoming hearings, we therefore encourage the Commission to consider at least the following topics.

**Lessons Learned from *Wyndham* and *LabMD*.** On privacy and data security matters, the Commission has hosted workshops,[5] issued reports[6] and entered into multiple consent decrees. But for all this informal guidance, there is still a dearth of formal guidance on how Section 5

[1] See, e.g., Tom Struble, "Resolving Cybersecurity Jurisdiction Between the FTC and FCC," *R Street Policy Study* No. 116, October 2017. https://goo.gl/yku1YH.
[2] See, e.g., Federal Trade Commission, "Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers," March 2012. https://goo.gl/M02JF3.
[3] See, e.g., Federal Trade Commission, "Privacy and Data Security Update: 2017," January 2017–December 2017. https://goo.gl/EJzRvx.
[4] See *LabMD, Inc. v. FTC*, No. 16-16270, slip op. (11th Cir. June 6, 2018). https://goo.gl/e5PZGC.
[5] See, e.g., Federal Trade Commission, "Informational Injury Workshop," Dec. 12, 2017. https://goo.gl/SjFxKz.
[6] See, e.g., "2012 Privacy Report."

applies to privacy and data security.[7] Indeed, despite having brought over 60 data security cases since 2002,[8] the Commission has only ever litigated three: *Wyndham*,[9] *LabMD*[10] and *D-Link*.[11] The first of these cases went in favor of the Commission,[12] but the second did not.

What should the Commission take away from these cases? The holding in *Wyndham* and dicta in *LabMD* suggest that privacy and data security are within the scope of Section 5 and that even in the absence of formal rules, the Commission can pursue these areas via case-by-case adjudication. However, the court in *LabMD* demanded more from the Commission's proposed remedy.[13] How will the Commission address the Eleventh Circuit's concerns going forward? Should the Commission's complaints and proposed remedies be more specific?[14] Should the Commission eschew behavioral remedies and pursue only monetary penalties?

**Informational Injuries and Civil Penalty Authority.** Last December, in an effort to better understand the various non-financial harms consumers can suffer when information about them is misused, the Commission hosted a workshop on informational injuries.[15] The intangible nature of these harms makes them difficult to detect and quantify, so it is understandable that the Commission has been struggling to deal with them. For example, the 2015 enforcement against Nomi Technologies strained the bounds of the Commission's Deception Policy Statement.[16] Instead of proving that Nomi's false promise of in-store opt-out mechanisms harmed consumers — because consumers would have chosen differently but for that deception — the Commission simply relied on the presumption that all express statements are material.[17] Such broad use of its deception authority is a poor way to pursue informational injuries, but there are also difficulties in using the Commission's unfairness authority.

---

[7] See, e.g., Justin (Gus) Hurwitz, "Data Security and the FTC's UnCommon Law," *Iowa Law Review* 101:3 (2016). https://goo.gl/pP6tAf; and Tom Struble, "Reforming the Federal Trade Commission Through Better Process," *R Street Policy Study No. 122*, December 2017. https://goo.gl/tEtBMN.

[8] 2017 Privacy and Data Security Update, p. 4.

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

[10] See *LabMD, Inc. v. FTC.* https://goo.gl/e5PZGC.

[11] See Federal Trade Commission, "FTC Charges D-Link Put Consumers' Privacy at Risk Due to the Inadequate Security of its Computer Routers and Cameras," Jan. 5, 2017. https://goo.gl/17qvYY.

[12] *Wyndham*, 799 F.3d at 249–59 (rejecting Wyndham's arguments that informal guidance alone cannot provide fair notice of what Section 5 requires in terms of data security).

[13] *LabMD*, at 25–31.

[14] See, e.g., Daniel Castro, "LabMD Ruling Gives FTC Chance for Course Correction on Cybersecurity," *Morning Consult*, June 13, 2018. https://goo.gl/2PHN5J.

[15] "Informational Injury Workshop." https://goo.gl/SjFxKz.

[16] Federal Trade Commission, "Complaint," In the Matter of NOMI TECHNOLOGIES, INC., Docket No. C-4538, Aug. 28, 2017. https://goo.gl/HbFLRf.

[17] See Federal Trade Commission, "Dissenting Statement of Joshua D. Wright, Commissioner," In the Matter of NOMI TECHNOLOGIES, INC., Docket No. C-4538, April 23, 2015. pp. 2–3. https://goo.gl/9hOxfy.

Indeed, in his recent testimony before the Senate, Chairman Simons admitted as much.[18] But the Commission's task is difficult, not impossible. The mere fact that "Section 5 does not provide for civil penalties,"[19] in some instances, does not leave the Commission helpless to pursue informational injuries. Section 5 does provide civil penalty authority for "knowing violations of rules and cease and desist orders respecting unfair or deceptive acts or practices[.]"[20] Thus, either a rulemaking under Section 18[21] or a fulsome body of case law would enable the Commission to file complaints and seek civil penalties even in cases where the degree of harm is difficult to quantify, as it often is with informational injuries.

Has the Commission considered undertaking a Mag-Moss rulemaking in this area? For example, could the Commission specify that maintaining inadequate data security, failing to post a privacy policy, or failing to notify affected users after a data breach are categorically unfair or deceptive practices? Are data breaches and other privacy incidents "prevalent" enough to satisfy the requirements of Section 18?[22] Could such a rulemaking provide the uniform national framework needed to preempt a patchwork of state privacy laws? Does the Commission have adequate resources on staff to manage such an undertaking? Should the Commission instead simply continue using its unfairness and deception authority to pursue informational injuries case by case?

* * *

R Street thanks the Federal Trade Commission for the opportunity to submit these comments, and recommends that the Commission pursue the above-identified areas in its ongoing work on promoting competition and innovation.

Respectfully submitted,

***/s/***

Tom Struble
*Tech Policy Manager*

R Street Institute
1212 New York Ave, NW
Suite 900
Washington, DC 20005
tstruble@rstreet.org

August 14, 2018

---

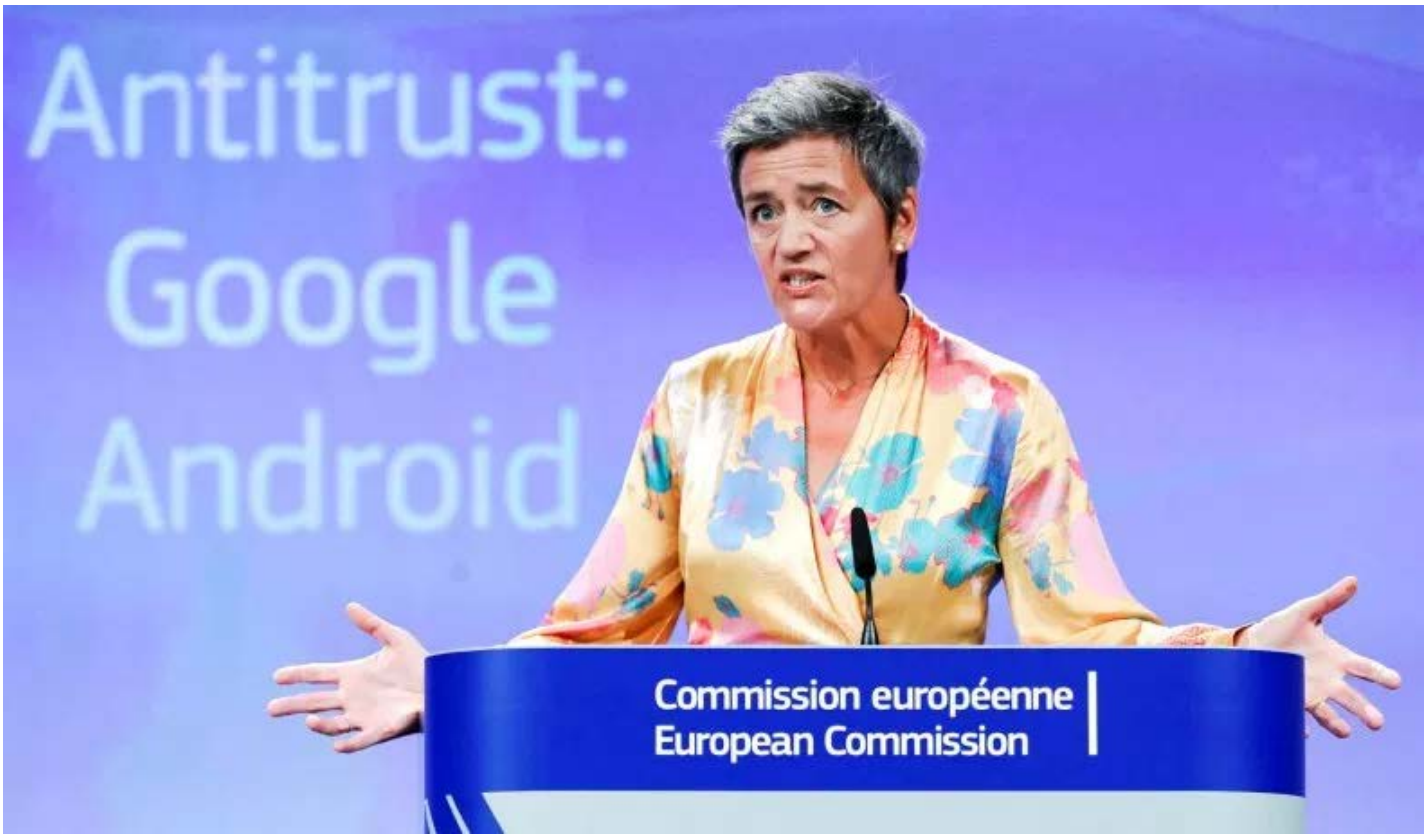
[18] Testimony of Joseph Simons, Chairman, Federal Trade Commission, House Subcommittee on Digital Commerce and Consumer Protection, "Prepared Statement of the Federal Trade Commission 'Oversight of the Federal Trade Commission,'" 115th Congress. July 18, 2018. https://goo.gl/abZVYp.
[19] Ibid., p. 6.
[20] 15 U.S.C. § 45(m).
[21] 15 U.S.C. § 57a.
[22] 15 U.S.C. § 57a(b)(3).

Fowler: Time to Buy a Round

ECONOMY & BUSINESS

# European Competition Law Is Hurting Consumers

By **TOM STRUBLE** | September 6, 2018 6:30 AM




European Competition Commissioner Margrethe Vestager at a news conference concerning Google in Brussels, Belgium, July 18, 2018. (Yves Herman/Reuters)

The EU's attack on Google is the latest salvo in an escalating war.

Antitrust law — or, as the rest of the world calls it, competition law — is designed to police unfair business practices that stifle competition and harm consumers. However, if done incorrectly, antitrust law can itself

Fowler: Time to Buy a Round

that far outweigh any associated harms.

Unfortunately, the Europeans seem to be getting it dreadfully wrong these days. Eager to protect small businesses (usually domestic) from their stronger competitors (usually foreign), the European Commission repeatedly intervenes in the market in ways that stifle competition, reduce innovation, and hurt consumers. Consider, for example, its recent case against Google.

In July, the European Commission fined Google over $5 billion for the way it licenses the Android mobile operating system to device manufacturers. The full text of the decision still hasn't been released, but the press release identifies three allegedly harmful practices: Tying Google's Search and Chrome apps to the Play Store in a software bundle; sharing Google's Search-app revenues with manufacturers who exclusively pre-install the app; and preventing manufacturers from offering both Android devices and devices that run on variations, or "forks," of the open-source Android operating system (such as Amazon's Fire OS, for example).

It's easy to see how these restrictions harm certain competitors in the mobile ecosystem, but it's also easy to see how they all benefit consumers. First, consider Google's tying practices.

Google ties the Play Store to its Search and Chrome apps in a bundle, so manufacturers who want the Play Store pre-installed on their Android devices must also pre-install the Chrome and Search apps. Manufacturers can also pre-install competing apps (such as Bing and Firefox), but Google's bundle ensures that any Android device with the Play Store also has at least one browser app and one search app pre-installed, allowing consumers to start using their new devices right out of the box without having to search for and download new apps. That's a clear benefit to consumers, but the European Commission has

Fowler: Time to Buy a Round

late 1990s.

**NOW WATCH:** 'Charges for Mail Bomb Suspect Have Been Announced'

When Microsoft was convicted of tying Internet Explorer to the Windows operating system in ways that stifled competition from alternative browser apps (such as Netscape Navigator), the remedy wasn't to prohibit the tying — Windows still comes bundled with Internet Explorer — but simply to prohibit Microsoft from using licensing or software restrictions that make it difficult or even impossible for users to switch to alternatives.

Google was one of the primary beneficiaries of that case — Chrome has now displaced Internet Explorer as the most popular web browser — and it intentionally designed Android to avoid antitrust liability by making it the most open, flexible, and differentiated platform in the world. That's why it's triflingly easy for Android users to uninstall or disable existing apps and switch to alternatives. Breaking apart Google's software bundle won't give consumers any

Fowler: Time to Buy a Round

Chrome and Search apps forced Google to start charging licensing fees for Android in order to cover its software-development costs) and more difficult to set up and use (if manufacturers either pre-installed no browser or search apps or pre-installed apps that were inferior to Google's). That seems like a net loss for consumers.

The commission's complaint over exclusive pre-installation and revenue sharing is similarly misguided. Manufacturers are already allowed to pre-install applications that compete with Google's apps and to pursue revenue-sharing deals with those competing application providers in exchange for pre-installation. However, Google offered manufacturers a share of the revenue generated via the Google apps on their devices if they agreed not to pre-install competing apps alongside Google's. The commission found that practice illegal because it harms competition among application developers, but consider the effects this will have on the rest of the market. Prohibiting revenue-sharing deals between Google and Android manufacturers may benefit competing application developers, but at the expense of both manufacturers (as access to that source of revenue is cut off) and, more important, consumers (as manufacturers raise device prices to make up for that lost revenue). That also seems like a net harm to consumer welfare, but this is what passes for competition law in the EU.

And finally, consider the commission's complaint over forking. Giving manufacturers complete freedom to both use and fork Android as they wish may help them differentiate their products and services, which could boost competition among device manufacturers. However, such fragmentation would come at an immense cost to consumers (who may be confused about subtle differences between devices running Android and Android forks) and to app developers (who would have to do extra work in order to ensure compatibility of their apps across additional operating systems). Historical evidence with Unix,

Fowler: Time to Buy a Round

Google could prevent harmful fragmentation in other ways. There is no mention, however, of just how effective these alternative anti-fragmentation strategies may be, or of how costly they would be to implement.

In failing to account for these costs, the commission has lost the plot and elevated competitors' welfare over that of consumers. Unsurprisingly, many are now questioning Europeans' motives — and not for the first time either. Claims that European competition law is just thinly veiled protectionism stretch back at least to the early 2000s, when the commission unilaterally blocked General Electric's acquisition of Honeywell — a combination that would have threatened domestic firms such as Airbus and Siemens. However, these claims have grown louder in recent years as the number of enforcements and severity of penalties brought against foreign firms have both increased. Even President Trump has taken notice.

Whether European competition law and the recently implemented General Data Protection Regulation (GDPR) truly are mercantilist policies designed to fleece foreign businesses and protect domestic firms is up for debate, but they do fit the pattern of an undeclared trade war. The commission's recent move to block Apple's takeover of Shazam does, too, since the primary beneficiary seems to be Stockholm-based Spotify. And this could all be just the beginning. Whatever their intentions, it will ultimately be consumers who wind up paying the price.

A recent study from Thibault Schrepel explained this point, showing how European competition law dramatically slows the pace of innovation by curtailing sanctioned firms' investments in research and development. Again, hobbling bigger and stronger rivals will benefit firms that are less efficient and less profitable, but it hurts consumers by discouraging fair competition, raising prices, and slowing the pace of innovation. And that, ultimately, is what's wrong with European competition policy. As Senator Mike Lee observed, "appropriate

Fowler: Time to Buy a Round

soon our European friends will realize that fundamental truth, because their current version of competition policy is hurting consumers.

**TOM STRUBLE** — Tom Struble is technology-policy manager and counsel with the R Street Institute, where he leads R Street's work on telecom, antitrust, and consumer-privacy issues.

75 | R Street Institute

## Fowler: Time to Buy a Round

Free markets. Real solutions.

R STREET POLICY STUDY NO. 153
October 2018

# REDUCING ENTRY BARRIERS IN THE DEVELOPMENT AND APPLICATION OF AI

Caleb Watney

CONTENTS



## INTRODUCTION

Artificial Intelligence (AI) is developing rapidly and countries from around the globe are beginning to articulate national strategies for handling the political ramifications.[1] Powering innovations like driverless cars, autonomous drones, full-sequence genetic analytics and powerful voice assistant technology, the future certainly looks full of potential.[2] However unsettled questions about who will reap these benefits and when they will be achieved leave storm clouds on the political horizon. Amid questions of industrial concentration and economic inequality on one side,[3] and concerns about lagging U.S. productivity and the slow pace of AI diffusion on the other,[4] this paper attempts to lay out a framework that can begin to address these various issues.

The first of these questions could be simplified to ask: what if only Google, Amazon, Facebook and Apple (GAFA) are able to develop the AI system that powers the economy of the future? The second considers the reasons that AI techniques have diffused through the economy at such a slow rate. However, although these appear to be two distinct questions, there is an under-examined overlap that connects these issues to the same set of policies: namely, high barriers to entry due to supply- side constraints.

There are significant barriers to entry in AI development and application, many of which stem from the direct result of government policies. These barriers have inadvertently boosted the market power of incumbent firms and thus in reducing them, we may enable new firms to better compete, while also removing some of the bottlenecks that slow down research and integration of AI systems across the entire economy.

Accordingly, the present study provides an overview of the various inputs to the production function of AI and analyzes the policies that should be reconsidered or implemented to reduce these barriers. Specifically, it will focus on the inputs of skilled AI analysts, high-quality datasets and specialized AI hardware. It will conclude with a short discussion of the relative attractiveness of focusing on entry barriers when

1. See, e.g., Tim Dutton, "An Overview of National AI Strategies," *Politics + AI*, June 28, 2018. https://medium.com/politics-ai/an-overview-of-national-ai-strategies-2a70ec6edfd.

2. For the exciting potential of AI in speeding the rate of economic growth and innovation, see, e.g., Iain Cockburn et al., "The Impact of Artificial Intelligence on Innovation," *National Bureau of Economic Research Working Paper* No. 24449, March 2018. http://www.nber.org/papers/w24449.

3. See, e.g., Kai-Fu Lee, "The Real Threat of Artificial Intelligence," *The New York Times*, June 24, 2017. https://www.nytimes.com/2017/06/24/opinion/sunday/artificial-intelligence-economic-inequality.html.

4. Erik Brynjolfsson, "Artificial Intelligence and the Modern Productivity Paradox: A Clash of Expectations and Statistics," *National Bureau of Economic Research Working Paper* No. 24001, November 2017. http://www.nber.org/papers/w24001.

compared to the high-risk options presented by traditional antitrust enforcement. While there are certainly other potential policies or AI inputs that are beyond the scope of this paper, the policy framework presented herein will nevertheless provide a useful primer for future analysis.

## A NOTE ON TERMS

At the outset, it is helpful to define a few specific terms that are applied in the following analysis. "AI" is meant to refer broadly to the set of computer algorithms being used to automate or improve aspects of human decision-making.[5] In the most current iteration, this is largely being accomplished via machine learning (ML), whereby an algorithm uses statistical techniques to progressively improve prediction ability for a given task.[6] By this definition, AI exists on a spectrum rather than as a binary, with increasing sophistication in the ability to apply various models to solve the problem at hand indicating higher levels of intelligence.

The term "AI development" refers to the research process of creating more advanced algorithms on the technological frontier. By contrast, "AI application" denotes the implementation of AI systems that have already been developed to new industries and problems. Development is vital for advancement in the field, while application is necessary for those advancements to actually affect the economy.

## SUPPLY OF SKILLED AI ANALYSTS

Perhaps the single biggest bottleneck in AI development and application today is the supply of skilled data scientists and machine-learning engineers. Typical AI specialists can expect to earn between $300,000 and $500,000 at top tech firms; numbers that are significantly higher than their peers in other computer-science-related subfields.[7] In addition to these ballooning salaries, industry experts like Hal Varian have pointed to the scarcity of adequate AI talent as the largest factor behind slow application in the economy.[8]

While the number of individuals pursuing careers as skilled AI analysts has certainly been increasing, the length of time it takes to develop necessary technical skills and the surging demand for AI specialists have created an intense labor shortage that benefits large, established firms. When bidding against deep-pocketed incumbents who can afford to pay the high six-figure salaries required to be competitive, it is difficult for startups and smaller businesses to compete for limited talent.[9] Similarly, given the costs of acquiring a skilled team for AI application, even established firms in non-tech sectors that may be able to afford high compensation will face a high bar to experimentation. So long as AI talent is sufficiently limited, it seems likely that the existing supply will be funneled primarily toward development rather than application.

For this reason, if there were appropriate policy levers to increase the supply of skilled technical workers available in the United States, it would disproportionately benefit smaller companies and startups. This would make the overall ecosystem more competitive while simultaneously increasing the rate of AI diffusion in other industries. To accomplish this, the following proposals should be considered.

### Reform our immigration system to allow more high-skill AI talent

The policy lever with perhaps the highest degree of leverage to begin immediately alleviating this talent shortage is our immigration system and more specifically, reform around visas for international graduate students.

In 2015, the United States had 58,000 graduate students in computer science fields, the overwhelming majority of which (79%) were international.[10] This represents a significant portion of the overall AI talent supply being cultivated each year, as students from all over the world are attracted to the nation's top education system. In particular, the United States attracts large numbers of students from China and India.[11] However, due to a limited number of visa slots, only a fraction of these students is allowed to work in the country long term.[12]

The primary pathway for these highly skilled immigrants to stay in the country is through the H-1B visa program.[13] However, for the past 16 years, the H-1B limit has been exhausted and, in more recent years, the number of applications filed has consistently been twice as high as the number of avail-

5. While definitions of AI vary, for an overview, see Peter Stone et al., "Artificial Intelligence and Life in 2030: One Hundred Year Study on Artificial Intelligence: Report of the 2015-2016 Study Panel," *Stanford University*, September 2016. p. 12. https://ai100.stanford.edu/2016-report.

6. Ibid, pp 2-4.

7. Cade Metz, "Tech Giants Are Paying Huge Salaries for Scarce A.I. Talent," *The New York Times*, Oct. 22, 2017. https://www.nytimes.com/2017/10/22/technology/artificial-intelligence-experts-salaries.html.

8. Hal Varian, *The Economics of Artificial Intelligence: An Agenda* (University of Chicago Press, Forthcoming), p. 20. http://www.nber.org/chapters/c14017.pdf.

9. See e.g., Michelle Cheng, "How Startups Are Grappling With the Artificial Intelligence Talent Hiring Frenzy," *Inc.*, May 25, 2018. https://www.inc.com/michelle-cheng/how-startups-are-grappling-with-artificial-intelligence-talent-hiring-frenzy.html.

10. "The Importance of International Students to American Science and Engineering," National Foundation for American Policy, October 2017. http://nfap.com/wp-content/uploads/2017/10/The-Importance-of-International-Students.NFAP-Policy-Brief.October-20171.pdf.

11. Ibid, p. 14.

12. "H-1B Visas by the Numbers: 2017-2018," National Foundation for American Policy, April 2018. https://nfap.com/wp-content/uploads/2018/04/H-1B-Visas-By-The-Number-FY-2017.NFAP-Policy-Brief.April-2018.pdf.

13. Ibid.

able spots.[14] And this is almost certainly understating the scope of the problem, as it does not account for the ways in which foreknowledge about the difficulty of acquiring a work visa may deter students from applying in the first place.

Although it also limits the talent pool available to large tech firms, the status quo is especially daunting for startups, as they do not have the specialized Human Resources personnel to handle the bureaucracy of the immigration visa application process. Including application and attorney fees, to sponsor a work visa typically costs around $5,000 per employee[15] and the paperwork burdens appear to be increasing.[16] Both the financial and bureaucratic costs are easier for established firms to bear, given their larger size and increased resources.[17]

In turn, this impacts the types of firms high-skill immigrants will apply to work for in the first place. Even when attracted to work at startups, foreign workers may ultimately privilege their applications to incumbents because they will likely have a better chance of obtaining work visas at established firms. Additionally, since startups face high failure rates, job loss could mean termination of work authorization as well. This would mean that the entire visa application process would have to be approached anew. Indeed, a recent longitudinal survey concluded:

> *Although foreign [STEM PhD students] are 45% more likely to be interested in working in a startup prior to graduation [when compared to US students], after graduation they are 50% less likely to do so. Controlling for ability and other characteristics, ex ante career interests are a strong predictor of startup employment among U.S. workers but not among foreign workers, suggesting that foreign workers may face constraints in choosing their preferred jobs [...] suggesting a potential pool of entrepreneurial labor that might move to startups if provided the opportunity to do so.*[18]

Accordingly, to allow more international students to live and work in the United States upon completion of their degree—either through an expansion and simplification of the H-1B visa program or through the creation of a new technical worker visa program—would be a relatively straightforward and effective method to alleviate the country's talent shortage around AI. In particular, this would benefit smaller firms and startups that are unable to access existing foreign-born talent to the same degree as established firms.

## Allow companies to deduct the cost of training AI talent

In addition to reforming our immigration pathways for high-skilled AI talent, it would be wise for the United States to extend more effort toward building up domestic talent. However, given that it can take years to train new AI specialists when compared with the near-instant effect of allowing already-trained, foreign-born experts to stay in the country, this will likely require a longer timeframe for the resources spent on this approach to pay off.

As the number of newly minted machine learning PhD students continues to dwindle, some companies are looking at training employees internally to essentially create new supply.[19] However, it requires significant investment on the company's part, both in time and resources, to train new AI specialists this way, and the gains from this training are mostly captured by the newly trained worker in the form of higher wages. In light of this and since workers can jump ship from the companies that train them at any time for a higher salary at a competitor, employers have few opportunities to recoup the costs of worker training.[20] It thus seems likely that employers are generally underinvesting in worker training when compared to the amount that might otherwise be efficient. We should therefore look more closely at incentivizing this socially desirable behavior through the tax code.

Employers may currently deduct a portion of the costs of worker training as long as it is to improve productivity in a role they already occupy, but this credit is fairly small and employers may not deduct the costs if it would qualify them for a new trade or business.[21] Expanding this deduction—both in size and scope—so that the full cost of worker training for new trades could be deducted, would incentivize more investment in building the AI workforce that is needed

14. Ibid, p. 2.

15. Matt Faustman, "How Much Will Sponsoring an H1-B Visa Cost an Employer?", *Upcounsel Blog*, 2013. https://www.upcounsel.com/blog/what-is-the-costs-for-an-employer-to-sponsor-an-h1b-visa.

16. Ana Campoy, "Trump is quietly swamping visa applicants in extra paperwork," *Quartz*, Jan. 11, 2018. https://qz.com/1176576/h1b-visa-under-trump-is-already-harder-to-get.

17. Jana Kasperkevic, "Getting an H-1B visa is becoming more difficult," *Marketplace*, April 2, 2018. https://www.marketplace.org/2018/03/30/business/immigration-reform-affect-businesses-hiring-visa-workers.

18. Cited with permission from Michael Roach et al., DRAFT: "U.S. Immigration Policies and the STEM Entrepreneurial Workforce," National Bureau of Economic Research, April 2018. http://www.nber.org/chapters/c14101.pdf.

19. "So we invite folks from around Google to come and spend six months embedded with the machine learning team, sitting right next to a mentor, working on machine learning for six months, doing some project, getting it launched and learning a lot." See, Steven Levy, "How Google is Remaking itself as a 'Machine Learning First' Company," *Wired*, June 22, 2016. https://www.wired.com/2016/06/how-google-is-remaking-itself-as-a-machine-learning-first-company.

20. See e.g., Alastair Fitzpayne and Ethan Pollack, "Worker Training Tax Credit: Promoting Employer Investments in the Workforce," The Aspen Institute, May 12, 2017. https://www.aspeninstitute.org/publications/worker-training-tax-credit-promoting-greater-employer-investments-in-the-workforce.

21. Michael Farren, "Bridging the Skills Gap," Congressional Testimony before the House Small Business Committee, Subcommittee on Economic Growth, Tax, and Capital Access, Examining the Small Business Labor Market, Sept. 7, 2017. https://www.mercatus.org/system/files/farren_-_testimony_-_bridging_the_skills_gap_-_v2.pdf.

to fuel our economy.[22] Given the pre-existing level of interest by employers in this strategy, it seems likely this could become a fruitful part of our domestic AI pipeline, if given more support.

Another way to frame this issue is by comparing the incentives for investment in worker training with those in other areas. For example, unlike investments in human capital development, investment expenditures for capital goods—like factories or robots—are currently fully deductible in the tax code.[23] This creates a system that incentivizes employers to invest more in capital productivity gains rather than labor productivity gains, which should be equalized to create a fairer playing field.[24]

As a simple example of a way in which this change could increase the supply of AI talent and speed AI diffusion, consider a hypothetical owner of a manufacturing plant. This owner has information technology (IT) staff who are generally technologically competent, but possess no special training in machine learning. She might be interested in sending this staff to a six-month, ML boot camp where they could learn the basics of applying ML techniques to analyze production processes and find new efficiencies in her manufacturing plant.[25] However, currently, such an expense would not be deductible, potentially discouraging her from making such an investment in the first place.

All else equal, allowing the costs of worker training to be fully deductible will spur more worker training. In the case of companies both developing AI and companies that could benefit from AI application, this means increasing the overall supply of skilled AI analysts in the economy. These workers will likely go on to use their skillsets for future employers, helping spur productivity growth and making the overall ecosystem more competitive.

## SUPPLY OF DATA

In many ways, the supply of high-quality machine-readable training data is the key enabler of machine learning. Without access to some underexplored dataset, a team of talented AI specialists can be left twiddling their thumbs. Consumer data in the United States is particularly valuable but large firms like GAFA have underlying digital services that supply them with immense reams of valuable and unique consumer data. Competitors do not easily have the same access.[26]

This is not inherently an issue, as these large technology companies have invested billions of dollars to create services that provide significant value for consumers and in return, consumers have shown a willingness to contribute their data.[27] We should aspire for other companies to create services that prove to create as much value for consumers. However, it is undoubtedly an advantage in particular domains of AI work that startups are currently unable to replicate.[28]

We should be careful to note, however, that beyond a certain threshold, increases in the sheer volume of data possessed generate decreasing returns to scale.[29] This means that while possessing high-quality data is vital for performance, simply having more data than a competitor is no guarantee of victory.[30] In fact, we are seeing that the role of sophisticated algorithmic design and ML feedback loops is only increasing.[31] Sometimes a smaller competitor with an adequate dataset and insightful algorithmic design can outperform an incumbent with a superior dataset but mediocre design.

Given all this, we can potentially create high-leverage opportunities for startups to compete against established firms if we can increase the supply of high-quality datasets available to the public. As with increasing the supply of AI talent, this will help both incumbents and startups but on the margin, it will be the smaller firms with less access to consumer data who benefit most.

22. In economic terms, an externality refers to a side effect or consequence of private sector action for which the effects are not fully reflected in the cost of the good or service. In this case, the positive effects of increased AI-talent supply for the entire economy are not fully internalized by the companies individually training workers. For this reason, many may generally be undersupplied.

23. See e.g., Gabriel Horwitz, "How The Government Perversely Encourages Machine Over Human Capital," *Forbes*, March 28, 2017. https://www.forbes.com/sites/washingtonbytes/2017/03/28/how-the-government-perversely-encourages-physical-over-human-capital/#23016623f9c6.

24. Some commenters have argued that to fully equalize the playing field between capital and labor improvement would require full-fledged, human-capital tax credits, similar to research and development tax credits. See, e.g., Rui Costa et al., "Investing in People: The Case for Human Capital Tax Credits," Centre for Economic Performance, Paper ISO1, February 2018. http://cep.lse.ac.uk/pubs/download/is01.pdf.

25. As an example of the type of programs more employers might take advantage of if the expense was tax deductible, see e.g., Austin Allred, *Twitter*, Sept. 12, 2018. https://twitter.com/AustenAllred/status/1039921578904043520

26. See e.g., Doug Aley, "It's Hard to Compete With Tech Giants Like Google and Amazon—But It Can Be Done," *Entrepreneur*, July 18, 2018. https://www.entrepreneur.com/article/316376.

27. Erik Brynjolfsson et al., "Using Massive Online Choice Experiments to Measure Changes in Well-being," *National Bureau of Economic Research Working Paper* No. 24514, April 2018. http://www.nber.org/papers/w24514.

28. See, e.g., Tom Simonite, "AI and 'Enormous Data' Could Make Tech Giants Harder to Topple," *Wired*, July 13, 2017. https://www.wired.com/story/ai-and-enormous-data-could-make-tech-giants-harder-to-topple.

29. For each piece of data accumulated, the amount of predictive power acquired decreases. See, e.g., "Stanford Dogs Dataset," Stanford University, 2011. http://vision.stanford.edu/aditya86/ImageNetDogs.

30. See, e.g., Joe Kennedy, "The Myth of Data Monopoly: Why Antitrust Concerns About Data Are Overblown," Information Technology and Innovation Foundation, March 2017. http://www2.itif.org/2017-data-competition.pdf.

31. See, e.g., Xavier Amatriain, "In Machine Learning, What is Better: More Data or better Algorithms," *KDnuggets*, June 2015. https://www.kdnuggets.com/2015/06/machine-learning-more-data-better-algorithms.html.

## Encourage the creation of open datasets and data sharing

One of the easiest ways to begin this process would be a more thorough examination of existing government datasets that are not public. As an example of previous projects that were broadly successful, consider the U.S. National Oceanic and Atmospheric Administration (NOAA) and Landsat projects, both of which made weather-satellite data available to the public and, in turn, developed into a multi-billion-dollar industry, creating more accurate forecasts of extreme weather and crop patterns.[32]

There appears to be even more potential from datasets the government owns but has not made public. For example, many cities and municipalities have useful data around traffic patterns, electricity usage and business development that, if made accessible, could lead to reduced-cost service provision and better analytics.[33] And there have been a flurry of recent pushes in Congress to standardize the publication of government agency datasets in a machine-readable format.[34]

It is frequently difficult to know beforehand how new data will be leveraged by startups and what new industries might form around it. After all, when the U.S. Government first made GPS-satellite data available to the public, they had no idea it would eventually become the backbone for location-tracking services used in smartphones around the world.[35] This should lead to a general presumption in favor of releasing government data, even if the consumer applications do not appear immediately obvious.

While there has been some concern around the privacy implications of making more government data public, especially data that might become personally identifiable, recent advances in data anonymization techniques like differential privacy should lessen these concerns.[36] While there may still be data that would be inappropriate to release to the public for national security or privacy reasons, it appears there is still significant progress to be made at current margins.[37]

There is also the matter of industries in which open data might become the norm if existing regulations are relaxed or streamlined. The healthcare industry seems a particularly promising target in this respect, as HIPAA has long been considered a barrier to the development of data sharing between medical professionals and companies.[38] Allowing consumer health data to be more easily shared with the proper privacy safeguards could enable a renaissance in drug development and personalized medicine, as recent ML advances have proven quite promising when appropriate data have been available.[39]

Each new dataset that can be easily shared or, when appropriate, made public, increases the odds both that a new startup will be able to leverage it for success, and also that a new industry can thrive around the increased predictive analysis the released data has enabled. For recent advances in AI to diffuse throughout the economy, we must make sure the underlying data is accessible.[40]

## Clarify the fair-use exemption for training data

In addition to making more government datasets open source, we should also take a second look at some of the intellectual property laws that intersect and interact with the ML process, specifically copyright law.

Imagine a hypothetical startup focused on the creation of a natural-language-processing application. One readily available source of human dialogue the company might consider learning from would be the last 50 years of Hollywood scripts, many of which are scrapable from various online databases. However, such an endeavor would stand on legally dubious grounds, as these scripts remain copyrighted works and there have not been clear legal guidelines established to delineate what is allowable as fair use in ML training data. Given this, it is more likely that such a startup would avoid

32. See, e.g., Christina Rogawski et al., "NOAA Open Data Portal: Creating a New Industry Through Access to Weather Data," *Open Data's Impact*, January 2016. http://odimpact.org/files/case-studies-noaa.pdf; and Tom Lee, "Closing Landsat data is (still) a bad idea," *Medium*, Aug. 9, 2018. https://medium.com/@thomas.j.lee/closing-landsat-data-is-still-a-bad-idea-8ef0ccfcc7dc.

33. See, e.g., Michael Chui et al., "Innovation in Local Government: Open Data and Information Technology," McKinsey Global Institute, 2014. https://goo.gl/wfSsro.

34. See, e.g., S.2852, "OPEN Government Data Act," 114th Congress, April 26, 2016. https://www.congress.gov/bill/114th-congress/senate-bill/2852.

35. Andrew Young et al., "United States GPS System: Creating a Global Public Utility," *Open Data's Impact*, January 2016. http://odimpact.org/files/case-studies-gps.pdf.

36. See, e.g., Kobbi Nissim et al., "Differential Privacy: A Primer for a Non-technical Audience (Preliminary Version)," *Vanderbilt Journal of Entertainment and Technology Law*, April 13, 2018. https://privacytools.seas.harvard.edu/publications/differential-privacy-primer-non-technical-audience-preliminary-version.

37. For more case studies of successful open-data initiatives and lessons learned, see Stefaan Verhulst and Andrew Young, "When Demand and Supply Meet: Key Findings of the Open Data Impact Case Studies," *Open Data's Impact*, March 2016. http://odimpact.org/files/open-data-impact-key-findings.pdf.

38. Niam Yaraghi, "To Foster Information Exchange, Revise HIPAA and HITECH," *Health Affairs*, Sept. 19, 2017. https://www.healthaffairs.org/do/10.1377/hblog20170919.062032/full.

39. See, e.g., Rob Matheson, "Artificial intelligence model 'learns' from patient data to make cancer treatment less toxic," *MIT News Office*, Aug. 9, 2018. http://news.mit.edu/2018/artificial-intelligence-model-learns-patient-data-cancer-treatment-less-toxic-0810; and Dave Gershgorn, "If AI is going to be the world's doctor, it needs better textbooks," *Quartz*, Sept. 6, 2018. https://qz.com/1367177/if-ai-is-going-to-be-the-worlds-doctor-it-needs-better-textbooks.

40. Note that this would also imply that new overly restrictive privacy laws could have the effect of raising barriers to entry and slowing innovation. Indeed, empirical evidence to date would appear to confirm this. See, e.g., Ajay Agrawal et al., "Economic Policy for Artificial Intelligence," *National Bureau of Economic Research Working Paper* No. 24690, June 2018, pp. 9-10. http://www.nber.org/papers/w24690.

this potential legal minefield and consider what other datasets might be available with less risk.

This is the ambiguous state of copyright enforcement in ML today. Legal scholar Amanda Levendowski has argued that this de facto privileging of frequently low-quality data that exists in the public domain (like the Enron emails) has inadvertently biased the many AI applications that are built upon them.[41]

However, this may also have important and underexplored applications for the state of competition. There are an enormous number of copyrighted works that are scrapable from the Internet, the data of which is currently underexploited in part because of its legally dubious standing if used as training data. This could represent, then, a significant lever to create new arbitrage opportunities for scrappy startups willing to find and leverage interesting datasets. The full scope of what this might entail or lead to is admittedly difficult to fully grasp, considering the massive amount of data that might be included.

Google has already showcased one use case for which this type of data might be leveraged. In 2016, a research division within Google used a collection of 11,000 free e-books to show the potential improvements that could be made to a conversational AI program.[42] This sparked considerable controversy with groups like the Authors Guild who considered it a violation of the author's intended purpose and argued it was a copyright violation.[43] Because this was a research paper and not publicly used for later commercial purposes, no suit was pursued. Notably, however, the original "BookCorpus" dataset is no longer publicly hosted.[44]

Given the existing ambiguity around the issue and the large potential benefits to be reaped, further study and clarification of the legal status of training data in copyright law should be a top priority when considering new ways to boost the prospects of competition and innovation in the AI space.[45]

## ACCESS TO SPECIALIZED HARDWARE

Underlying the data being used to train ML models and the data scientists who are building them is the physical infrastructure of the AI world. This primarily takes the form of the computer servers and chipsets that ML models are trained and operated on. In recent years, this hardware has become increasingly specialized to keep up with the pace of AI development. As the tasks asked of various ML systems continue to diverge, the type of computational power enabled by specific chip architectures has become just as important as the sheer magnitude.

As AI scholar Tim Hwang has noted, there are two dynamics that are shaping the marketplace for ML hardware today.[46] The first is the inverse relationship between performance and flexibility or in other words, that general purpose hardware that tends to be less expensive and is used for a wide variety of computing tasks is being outpaced in performance by chipsets built for a specific task.[47] The second dynamic pertains to the differing types of hardware used for initial training of an ML model and for making inferences with an already-trained model.[48] For example, energy consumption for a computer-vision system may matter a great deal when operating on a mobile phone, but not when the model is originally being trained in a data center. As Hwang concludes: "These considerations influence what kinds of hardware are used at which points in the lifecycle of a machine learning system. They can be viewed as separate though overlapping markets, with hardware platforms being offered either for training or inference, and some offering support for both."[49]

While a natural and necessary part of the AI development process, such a trend toward specialized hardware does increase the fixed costs required to be competitive. This manifests not only in the expense of these systems, but in the elaborate supply chains that have been built up to support them. While the policy recommendations that flow out of this insight are less clear cut than those for the supply of AI analysts or datasets, maintaining access to valuable AI hardware is a key policy consideration.

### Avoid causing political instability to international supply chains

As AI hardware becomes more specialized, the supply chains for very specific chips become a critical ingredient for cutting-edge ML research. While the United States maintains advanced manufacturing facilities that are vital to the sup-

41. Amanda Levendowski, "How Copyright Law Can Fix Artificial Intelligence's Implicit Bias Problem," *Washington Law Review* 93 (July 19, 2018), pp. 579-631. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3024938.

42. Samuel R. Bowman et al., "Generating Sentences from a Continuous Space," Google Brain, May 12, 2016. https://arxiv.org/pdf/1511.06349v4.pdf.

43. See, e.g., Richard Lea, "Google swallows 11,000 novels to improve AI's conversation," *The Guardian*, Sept. 28, 2016. https://www.theguardian.com/books/2016/sep/28/google-swallows-11000-novels-to-improve-ais-conversation.

44. See, for example, this GitHub forum discussion about the missing 'BookCorpus' dataset and the encouragement to scrape the data again oneself. https://github.com/ryankiros/neural-storyteller/issues/17.

45. For a more critical examination of the potential problems with expanding the scope of fair use in machine-learning training data, see Benjamin Sobel, "Artificial Intelligence's Fair Use Crisis," *Columbia Journal of Law & the Arts*, Forthcoming. https://ssrn.com/abstract=3032076.

46. Tim Hwang, "Computational Power and the Social Impact of Artificial Intelligence," *MIT Media Lab*, March 23, 2018. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3147971.

47. Ibid., p. 8.

48. Ibid., p. 9.

49. Ibid.

ply chain, much of the production for particular parts (like semiconductor fabrication) have been outsourced. Given the importance of chip foundries in Taiwan and China in particular, the perceived stability of trade in the region will alter investment patterns and domestic access to these sophisticated chips.[50]

To ensure access in spite of political tensions, large companies like Apple, Google and Nvidia are beginning re-shore production of especially valuable chips.[51] However, smaller competitors and startups are much more limited in this capacity and thus are more reliant on existing international supply chains.

Insofar as recent U.S. trade tensions with China have increased the perceived instability of regional trade, the disparate impact this will have on smaller firms should be recognized.[52] Ultimately, new foundries and semiconductor manufacturing plants will shift wherever it is most profitable. Accordingly, in the event of a long-term trade war, production could eventually shift elsewhere. However, it will certainly shape short- and medium-term access to specialized hardware.

While this analysis has focused on the effects to domestic competition, the pros and cons of a coordinated national security push to on-shore semiconductor manufacturing are beyond the scope of this paper, but the effects of that decision could impact the degree to which this continues to be a meaningful issue.[53]

## Maintain a healthy ecosystem around distributed platforms

The other significant trend in AI hardware utilization is the growth of cloud-computing platforms like Amazon Web Services (AWS) and the Google Cloud platform. Cloud computing has notable pro-competitive effects in that it transforms what is normally a fixed cost in server capacity into a variable one.[54] Allowing a startup to buy only the discrete server space they will need for that month significantly reduces the amount of venture capital needed to get a company off the ground.

This becomes even more important as AI hardware becomes more specialized. Requiring a startup to buy different chips for the various life cycles of training and operating an ML algorithm would be a significant financial outlay and almost certainly hurt the ability of startups to compete. Fortunately, both AWS and Google Cloud have been competing with one another by adding specialized AI hardware as a part of their platform offerings.[55] This essentially allows startups to spread out the increased fixed costs of specialized hardware over a longer time horizon, which makes it more manageable.

In addition to the physical servers themselves, cloud computing companies are increasingly offering ML services like voice recognition, translation and image recognition to save startups the hassle of building their own software tools for each discrete task.[56] Again, it is difficult to understate how much easier this makes the process of launching a startup and it is a very positive development for the overall health of the AI ecosystem.[57]

This is closely related to the trend we have seen in the usage of distributed and open-software platforms like TensorFlow and GitHub, which provide ML platforms for startups to build, train and publish their software. While not hardware in the traditional sense, all of these can be thought of as a type of toolkit that exists around and supports the creation and development of AI. It is also noteworthy that many of these tools and platforms are effectively being developed and maintained for free by current incumbents.[58]

As this portion of the ecosystem largely seems to be developing in a healthy manner, the United States should be careful to avoid data-localization laws, excessive privacy laws, and other legislative efforts that might disrupt the careful balance.[59] On the whole, recommendations for this area should largely follow the Hippocratic Oath and "First, do no harm."

50. Ibid., pp. 18-21.

51. See, e.g., Reinhardt Krause, "In AI Technology Race, U.S. Chips May Be Ace-In-The-Hole Vs. China," *Investor's Business Daily*, Nov. 27, 2017. https://www.investors.com/news/technology/ai-technology-u-s-chip-stocks-vs-china; and Andy Patrizo, "The AI revolution has spawned a new chips arms race," *Ars Technica*, July 9, 2018. https://arstechnica.com/gadgets/2018/07/the-ai-revolution-has-spawned-a-new-chips-arms-race.

52. See, e.g., Ben Blan, "US-China trade war prompts rethink on supply chains," *Financial Times*, Sept. 3, 2018. https://www.ft.com/content/03e4f016-aa9a-11e8-94bd-cba20d67390c.

53. Hwang, pp. 29-32. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3147971.

54. Varian, p. 5. http://www.nber.org/chapters/c14017.pdf.

55. See, e.g., Cade Metz, "Google Makes Its Special A.I. Chips Available to Others," *The New York Times*, Feb. 12, 2018. https://www.nytimes.com/2018/02/12/technology/google-artificial-intelligence-chips.html.

56. Varian, p. 5. http://www.nber.org/chapters/c14017.pdf.

57. See, e.g., Kenji Kushida et al., "Diffusing the Cloud: Cloud Computing and Implications for Public Policy," *Journal of Industry, Competition and Trade* 11:3 (September 2011), pp 209-37. http://brie.berkeley.edu/publications/WP_197%20update%206.13.11.pdf.

58. While Google and Microsoft obviously benefit from the close developer relationships they maintain by offering TensorFlow and GitHub, it would be very difficult to argue the net effect of their existence is not pro-competitive.

59. See, e.g., Nigel Cory, "Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost?", Information Technology and Innovation Foundation, May 1, 2017. https://itif.org/publications/2017/05/01/cross-border-data-flows-where-are-barriers-and-what-do-they-cost.

## ANTITRUST CONSIDERATIONS

It is worth contrasting this general approach of reducing barriers to entry with another commonly cited remedy: stronger antitrust enforcement.[60] While concern over the level of domestic competition faced by GAFA is, of course, not unique to AI, it has certainly raised the stakes given how central the technology is to their current and future business models.

However, traditional antitrust measures may prove to be fairly difficult to implement and high risk for dealing with this perceived problem. After all, there are many plausible arguments supporting the current consolidated structure of the AI industry, particularly those that emphasize the importance of cross-cutting technical expertise, and the ability to leverage data and services from one business application to another.[61] While a full analysis of the antitrust implications of the AI industry is outside the scope of this paper, it is helpful to foreground the risks associated with such an approach.

If critics are right, breaking up or actively restricting the merger activities of large tech firms could lead to more innovation in the long run.[62] If these companies are indeed leveraging their significant market power to make it harder for startups to compete with them, breaking them up or constraining them could be a remedy.[63]

However, if critics are wrong about the optimal market structure of AI development and strong antitrust action is pursued, the consequences could be dire.[64] An increasing amount of evidence suggests that a small sliver of firms on the technological frontier have been responsible for the lion's share of productivity gains in the economy.[65] For this reason, breaking them up potentially risks killing the goose that lays the golden egg.[66]

By contrast, focusing on lower barriers to entry is a fairly low-risk strategy for injecting more competition into the AI landscape. If the United States can make it easier for startups to compete against large, established incumbents, it increases the likelihood of achieving the boosts to dynamism and innovation that antitrust advocates champion. Further, it would do so without risking the destruction of the current market equilibrium that is producing significant gains for consumers and for the broader economy. If GAFA can withstand the Schumpeterian winds[67] of increased competition from startups, it is all the better for them.

However, as this paper has documented, there are significant barriers to entry in AI development that have boosted the market power of incumbent firms. If, in the absence of these barriers, new startups can successfully compete, it will be a win for innovation, consumers and for the dynamism of the economy as a whole.

One reason this strategy is lower risk than traditional antitrust remedies is because it does not impose a specific vision of market efficiency from the top down. Rather, it increases the level of competition from the bottom up in the hopes of displacing incumbent firms, if—and only if—the new firms are indeed more productive.

Furthermore, even if the current market structure is the most efficient, reducing the identified barriers to entry will increase the overall rate of innovation in the market by allowing AI to be developed more quickly. This will also aid in the diffusion of AI application across the rest of the economy, spreading the significant productivity gains that can result. Finally, it will make the United States more competitive on the international stage, as we compete with other nations to establish ourselves as the best place to develop and deploy AI systems.[68]

Considering the stakes involved and the relatively low risk associated with reducing barriers to entry, policymakers would be wise to focus on this agenda before moving on to more heavy-handed and higher-risk alternatives. Even in the

60. See, e.g., Robert Wright, "Google Must Be Stopped Before It Becomes An AI Monopoly," *Wired*, Feb. 23, 2018. https://www.wired.com/story/google-artificial-intelligence-monopoly.

61. See, e.g., Will Rinehart, "Breaking Up Tech Companies Means Breaking Up Teams And The Underlying Technology," American Action Forum, July 23, 2018. https://www.americanactionforum.org/insight/breaking-up-tech-means-breaking-up-technology-and-teams.

62. Editorial Board, "Break Up Google," *The Boston Globe*, June 14, 2018. https://apps.bostonglobe.com/opinion/graphics/2018/06/break-google.

63. Lina Khan, "Amazon's Antitrust Paradox," *Yale Law Journal* 26:3 (2016), pp. 710-805. http://digitalcommons.law.yale.edu/ylj/vol126/iss3/3.

64. Will Rinehart, "Breaking Up Big Tech Is Hard to Do," *The Wall Street Journal*, July 22, 2018. https://www.wsj.com/articles/breaking-up-big-tech-is-hard-to-do-1532290123.

65. See, e.g., Dan Andrews et al., "Frontier Firms, Technology Diffusion and Public Policy: Micro Evidence From OECD Countries," Organization for Economic Co-operation and Development, 2015. https://www.oecd.org/eco/growth/Frontier-Firms-Technology-Diffusion-and-Public-Policy-Micro-Evidence-from-OECD-Countries.pdf. Also, note that these large tech companies are by far the largest spenders on research and development in the United States. See, e.g., Rani Molla, "Tech companies spend more on R&D than any other companies in the U.S.," *Recode*, Sept. 1, 2017. https://www.recode.net/2017/9/1/16236506/tech-amazon-apple-gdp-spending-productivity.

66. For more on the high-risk nature of traditional antitrust enforcement in this sector, see Geoffrey Manne and Joshua Wright, "Innovation and the Limits of Antitrust," *Journal of Competition Law and Economics* 6:1 (2010), pp. 153-202. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1578762.

67. The economist Joseph Schumpeter popularized the term "creative destruction" and describes the effect of competition as feeling like a "gale" that "incessantly revolutionizes the economic structure from within, incessantly destroying the old one, incessantly creating a new one." Joseph Schumpeter, *Capitalism, Socialism and Democracy* (Routledge, 1942), pp. 82–83.

68. For more on the importance of international competition in AI, see, e.g., Michael Horowitz et al., "Strategic Competition in an Era of Artificial Intelligence," Center for New American Security, July 25, 2018. https://www.cnas.org/publications/reports/strategic-competition-in-an-era-of-artificial-intelligence.

event that strong antitrust enforcement is eventually called upon, enabling a more competitive ecosystem beforehand could help reduce the scope of the problem.

## CONCLUSION

Artificial intelligence holds tremendous opportunity for our economy and for consumer benefit. However, the current barriers to entry in acquiring skilled talent and high-quality datasets may be impacting the number of startups that are able to compete successfully. And while the market for AI hardware appears to be developing in a healthy manner so far, policymakers should be careful not to implement policies that could backfire. To ensure a competitive and innovative ecosystem going forward, then, policymakers should prioritize reducing the barriers to entry as our first line of defense.

**ABOUT THE AUTHOR**

**Caleb Watney** is a technology policy fellow at the R Street Institute, where he leads the organization's work on emerging technologies, including autonomous vehicles, artificial intelligence, drones and robotics. He received his master's degree in economics from George Mason University.

OPINION

# Can BuzzFeed Save Us From Deep Fakes?

BY **JEFFREY WESTLING**
October 23, 2018

When looking for a hard-hitting, fact-checking reporter, the mind doesn't normally jump to a writer for BuzzFeed. Maybe it should.

Recently, a Facebook user and self-identified "competitive barefoot runner" wrote a post on a local community page complaining about acorns "littered" on the sidewalk. The post quickly went viral as others expressed predictable outrage, and in a rush to generate traffic, many news sources simply ran a story about the seemingly bizarre post and the outrage it generated in the community.

However, BuzzFeed took a deeper look into the claims — by calling the original poster — and broke the exclusive story: The whole thing was a fake.



"Just goes to show. You can't fool journalists, unless they are from the Washington Post or Esquire or Gizmodo or Fast Company or Upproxx," the author of the original post explained.

While the BuzzFeed investigation of competitive barefoot running may seem silly on its face, it is an important clue in answering how society can deal with much more serious challenges of technology-enabled disinformation — so-called "fake news."

The technological fabrication scheme du jour is the "deep fake": a class of simulated audiovisual materials that uses modern artificial intelligence algorithms to make animated content appear realistic — in other words, AI-generated fake videos of real people. The technology has advanced remarkably quickly of late, and because of the apparent realness of the final product, some worry that deep fakes will undermine elections or threaten national security. In other words, these commenters believe that deep fakes "will threaten to erode the trust necessary for democracy to function effectively" and are calling for legislation to stop their proliferation.

At the core of these critiques is the idea that the new technology represents an unprecedented challenge that requires an unprecedented response. But that is not entirely true.

While AI-generated fake video as a tool may be novel, society has faced similar challenges when handling deceptive media — and new technology used to create such media — in the past. And as this experience shows, society can rise to the challenge in minimizing the potential harms that new technology can present.

In the 1990s, news outlets and commentators made apocalyptic claims about the death of photography as new tools for digital editing, such as Adobe Photoshop, became commercially available. For example, a 1990 Newsweek article argued that "in the future, the Chinese or others with something to hide wouldn't even worry about photographers" because of the distrust of photographs.

We obviously do not live in that world of distrust today. But why? Many early attempts at digitally altering images left glaring imperfections in the product and resulted in controversial news coverage for the publication, making the public acutely aware of the new technology.

The market in turn responded to the pressures, with both news agencies and photojournalists imposing codes of ethics related to the editing of photographs for publication. While people still may be deceived by a well-done Photoshop image, photography continues to persist as a trusted and respected source of information when the context surrounding the photo supports its veracity.

The deep fakes of 2018 are obviously not the Photoshop of 1990, and the world is different enough that the same chain of events is unlikely to alleviate the deep fakes problem. Yet many of the same lessons we learned from the advent of photo-editing software can be applied to this new technology, and the worries associated with deep fakes will likewise fail to materialize.

That's where BuzzFeed comes in. New media outlets, along with sites such as PolitiFact and Snopes, already fact-check the statements of politicians and the stories of other news sources. Indeed, BuzzFeed itself made a conscious decision to move into investigative journalism — a strange choice for a site originally specializing in viral listicles — once it realized that there was a demand.

If the problems associated with the new technology are as serious as some worry, a new market for deep fake "fact-checkers" will likely open up. Obviously, a story about barefoot running and acorns littered on the sidewalk is much easier to debunk than a sophisticated, digitally altered video. However, the incentive for a

company like BuzzFeed to apply the same journalistic rigor to a viral deep fake video is similar to, or perhaps even greater than, the incentive to expose a fake post on Facebook.

Clearly, simply debunking deep fake videos can't solve the larger issue of fake news generally. But still, it highlights a key point: The market tends to adapt to new technologies and resolve what many expect to be the new challenges a given technology will present.

Furthermore, these solutions often take unexpected forms. Trying to regulate a technology at a specific point in time may foreclose the ability for innovative new services, such as a BuzzFeed fact-checker, to develop and enter the market.

So will BuzzFeed save us from deep fakes? Maybe, maybe not. But if history is any indication, the apocalyptic claims will likely fail to live up to the hype.

*Jeffrey Westling is a technology and innovation policy associate at the R Street Institute, a free-market think tank based in Washington, D.C.*

Morning Consult welcomes op-ed submissions on policy, politics and business strategy in our coverage areas. Updated submission guidelines can be found here.

BRANDS

89 | R Street Institute