Regulatory Transparency Project

Unlocking Innovation & Opportunity

Regulators in Cyberia

Cyber & Privacy Working Group

Stewart Baker
Thomas "Tom" Hazlett
Matthew R. Heiman (Chair)
Justin "Gus" Hurwitz
Jamil N. Jaffer
Paul Rosenzweig
Megan Stifel

This paper was the work of multiple authors. No assumption should be made that any or all of the views expressed are held by any individual author. In addition, the views expressed are those of the authors in their personal capacities and not in their official/professional capacities.

24 July 2017

Table of Contents

I. Executive Summary

This paper illustrates the negative and sometimes unintended consequences that regulations can have on America's most dynamic and fastest growing industry: the technology sector. In many situations, there is no regulatory option that satisfies Goldilocks' preference of being "just right" because the newness of the service or product makes it impossible to know what "just right" is.

Following the introduction, Section III provides a brief history of the development of the Internet and the technology sector that has taken wing. Contrary to what some believe, the Internet was neither the product of genius central planning in the bowels of Pentagon bunkers, nor was it the masterstroke of a former Vice President. Instead, the Internet was born because the needs of the government, academics, the private sector, and eventually consumers to connect systems to each other drove a consistent pattern of incremental innovation. In the span of fifty years, systems networked over distance have given rise to a new economy, all of which was incubated in an environment with little to no regulations.

Section IV explores what happens when new wine (the provision over the Internet of commercial services and learning platforms) is poured into old regulatory bottles (the Americans with Disabilities Act (the ADA), a 1990 vintage). The ADA prohibits discrimination against those with physical handicaps and mental impairments in public accommodations. This is the reason that public places generally have ramps, handicap accessible restroom stalls, and signage in Braille. The ADA never contemplated the Internet, but because there have been no revisions to the law or clarifications to the related regulations, plaintiffs have sued retailers, universities, and other businesses for not making websites accessible to those with visual or hearing impairments. Retailers most either spend money to make their sites comply, run the risk of operating in an unclear environment, or shut their sites down. Because of the costs of adding subtitles to videos of lectures, universities have removed such content from their websites. No loaf has trumped having a good part of the loaf.

Section V describes the obstacles that are faced by some of the most innovative and consumer-popular companies in the marketplace: Uber, Lyft, Airbnb, and Kickstarter, among others. Because these new companies threaten more traditional businesses (taxi cab companies, hotels, and banks) by providing consumers with greater service and pricing choices, the legacy competitors have responded by agitating municipalities and states to place the Internet upstarts in the regulatory penalty box, often on the basis of public safety and security. Despite the absence of significant passenger risk, regulatory demands in Austin, Texas forced Uber and Lyft to leave market for a year. Until a state law was enacted in June 2017 overruling a local ordinance, Austinites were forced to hail rides from legacy taxi operations – much the way the rest of the country did in 2000.

Unfortunately, as set forth in Section VI, regulations born of seemingly good intent can have a crippling effect on the vibrant cybersecurity industry. The Wassenaar Arrangement is an effort by many governments, including the U.S., to place export control restrictions on cybersecurity tools. These tools, which are critical to identifying vulnerabilities in information technology infrastructures owned by governments, companies, and public institutions, can also be used by hackers with bad intent or rogue states seeking to undermine democracies or suppress their own populations. Because these tools are used to address vulnerabilities that can arise in days or even hours, waiting on export licenses for weeks or months destroys their utility and hampers the growth and innovation of an industry that is critical for the future of our cyber defenses. Moreover, the hackers and authoritarian regimes will not worry about licenses. The group at greatest risk is the legitimate actors that wish to play by the rules, even those that are overbroad, ill-defined, and retard legitimate commerce.

Section VII looks at how the Federal Trade Commission (FTC), an agency given broad enforcement powers over unfair trade practices that affect consumers, can abuse its powers when there is insufficient judicial oversight. This is particularly true in the cyber and privacy sector where the FTC has brought over 200 regulatory enforcement actions. Because of the reputational harm, distraction, and cost of litigating these matters, many companies will settle with the FTC and sign a consent decree. Such agreements are not subject to oversight or review by courts. In some consent decrees, the FTC takes the view it should monitor the company for 20 years. In the life of the information economy, 20 years covers the birth, use, and death of multiple generations of a technology. Additionally, if a company wants to stay out of the FTC quagmire, it will struggle to do so because the FTC has issued very little guidance to articulate what "unfair" means.

The Internet of Things (IoT) is developing rapidly and represents the next wave of change in the technology sector. Section VIII reviews the challenge of using rigid, bureaucratic regulatory processes to oversee a sector that is changing every week. While certain regulation may be necessary, it will be important for regulators to act in a way they usually do not: with prudence, precision, modesty, flexibility, and restraint. Sometimes, the best response is to watch and wait.

The Conclusion of the paper offers some modest advice for regulators and the industry. Like the Hippocratic Oath, regulators first instinct should be to do no harm. The technology sector has generated and will continue to generate new solutions, new innovations, jobs, wealth, and a better quality of life for all if it is handled with care. The industry grew rapidly because it operated in a space with few rules or restrictions. We are all beneficiaries of that. While regulations provide certain social goods, outside of lobbying shops and law firms, they generally do not create jobs and unleash innovation. This means that regulators need to steal a page from the cyber innovators' playbook – start small, be transparent, and adjust as needed.

II. Introduction

> "It's a strange new place, this 'cyberspace'…. It is no-place, but it somehow seems to span the entire globe, and it keeps growing…"[1]

What is the role of Federal regulation and standard setting in the technology sector? Should government, for example, be responsible for mandating cybersecurity standards? Or will such rules stifle innovation and diminish economic benefit?

While these questions have economic, technical, and social dimensions, this paper addresses these questions principally from a legal perspective. Our conclusion is simple – regulation should be the Federal tool of last resort.

The American economy has historically been robust, compared to other major Western nations, due to a better climate for entrepreneurial activity. Over the past four decades or so, the technology sector has enjoyed rapid growth, with tremendous innovation across a wide-range of markets, in significant part because of the relative lack of regulation. Given freedom to create, innovators have introduced disruptive technologies from Silicon Valley and San Diego to New York City to Boston – and Austin, Texas, Nashville, Tennessee and Pittsburgh, Pennsylvania.

This is not to suggest that the technology industry, like others, could not benefit from incentives to promote beneficial behavior, nor that regulation may never be necessary. To the contrary, there are a wide range of social outcomes that policy makers might want to encourage. Some argue that in the area of security, the private sector fails to effectively policy itself and be responsible for the cost and harm caused by security failures. Observers argue that this failure to self-govern requires well-designed government policy actions.

Whether or not security is an example of the need for government policy, the best approach to obtaining potential benefits is typically with positive incentives (the "carrot") rather than reaching instinctively for the regulatory "stick." The positive approach improves transparency and tends to produce less collateral damage. With parties given incentives to create solutions, imaginative new approaches can improve outcomes while costly "unintended consequences" are avoided. From tax incentives to innovation grants, targeted rule changes, government purchasing, and direct investment, there are a wide range of positive tools at the government's disposal to obtain the products, services, and capabilities it needs from the nation's burgeoning technology sector. And these same tools can also help to set baseline government requirements and expectations for everything from corporate cybersecurity to internal product development standards and the like.

While the use of positive incentives may take longer to propagate through the economic system than the use of direct regulation, the reality is that positive incentives, particularly if deployed to a wide

[1] David G. Post, IN SEARCH OF JEFFERSON'S MOOSE: NOTES ON THE STATE OF CYBERSPACE (Oxford, 2009), at 3.

range of organizations and innovates, can have similar outcomes to direct regulation over the long run.

The danger of regulatory overreach in the technology sector is particularly strong. Regulations are inherently rigid. They involve lengthy administrative processes to create, modify, or remove. This reality makes it hard to engage in rapid course correction when needs change, perhaps – as endemically occurs in this sector – because an established business model has been disrupted or an underlying technology displaced. Rules which had been perceived as necessary remain stuck in time, fixed in place long past their usefulness. There they become impediments rather than expedients. More often than not, regulators would be wise to follow the advice, "Don't just do something, stand there."

Moore's Law and Regulatory Pace

Moore's Law: Processing power doubles every 18-24 months

Regulatory pace: Major rulemakings take roughly 2-3 years [Public Citizen]

Nevertheless, there are occasions when regulation is necessary. But the search for more efficient alternatives, specifically for policies that achieve the desired ends without locking in counter-productive barriers to innovation, should not therefore end. In successfully steering society's choice among the options, policy makers should consider all the relevant costs and benefits. This is crucial in the technology sector, where the potential for dynamic innovation can yield huge gains for economic development – and thereby produce large losses when unnecessary restrictions block them. With short-lived product cycles and waves of technological progress, heavy administrative processes will struggle to keep up. Regulators are not known for an innovative approach to seeking better, more efficient ways to regulate.

In an environment where the market is dynamic, this paper concludes that the best answer is a "do no harm" approach to the use of regulatory tools – general standards whose meaning evolves as technologies change. Even here, caution is necessary. We have already seen, for example, risible claims by an agency that it can, and should control market structures 20 years into the future (see Section VI). If we allow regulation to overreach we risk killing the economic engine of the network – to the detriment of everyone.

III. The Emergence and Growth of the Internet – A Brief History

The emergence of the Internet has wrought profound changes in the way people communicate. That, in turn, has disrupted economic markets, transformed social relationships, and challenged governments. It both inspires and frustrates, raising profound new opportunities as it renders old structures, customs, and manners obsolete. It is undeniably an amazing source of progress, unleashing new sources of knowledge and wealth. But, as with all great change, its potential relies heavily on how we receive and nurture such advances.

A. Early History

The history of this change is clouded by a good deal of folklore. The Department of Defense did not create the Internet to harden U.S. survivability in the event of a nuclear attack. Indeed, in the 1960s the Air Force did consider how a decentralized communications grid – distinct from the traditional telephone system – might operate. But, DoD terminated the research and took no action.[2] DoD's DARPA (Defense Advanced Research Projects Agency) contracted with private firms that created data links to connect computer facilities doing defense-related work. There was no vision for what's become today's Internet.

The basic communications mission was new: allowing computers to talk. With the existing telephone network pioneered by Alexander Graham Bell in the 1800s, two people would enjoy a conversation over electrical pathways dedicated to transmitting their voices. To link the parties, the circuits would be switched; in the classic example, the local phone operator (of which Lily Tomlin's comic impersonation is now our historical memory) would physically plug one line into another at a switchboard – "circuit switching."

When the task was to allow computers to "talk", key innovations emerged that dramatically altered network development. DARPA contracted with various companies to let researchers in distinct locations collaborate. In crafting this new system, concerned with transporting data rather than voice, new choices were made. Computer information was digitized – turned into bits, ones and zeros – and made uniform. These bits were bundled into packets; thousands of packets might form one message. But the packets did not need to travel together along the same path. The packets could scramble, find their best route (traveling at about the speed of light), and then be reassembled at the final destination.

The great advantage of this system was that no dedicated circuit was needed. That freed up vast capacity. Not only were the use of communications conduits now able to carry more, the standardization of bits and transport protocols made coordination across different networks, devices and applications easy. Various enterprises could build new lines, or concoct new content, and seamlessly plug in. This "inter-net" formed from a network of networks.

The New Industry

Yahoo! was an early web portal created by Stanford engineering students Jeffrey Kang and David Filo. In 1995, some $3 million was invested by venture capitalists. The value of the company rose with the boom and fell with the bust (following March 2000), but the firm survived.

Amazon started more conventionally. Book selling is a niche where large inventories are good, but huge inventories are better. The Internet, with its broad reach, enabled "the long tail." The retailing efficiencies soon went far beyond books. Launched in 1994, the company went public in 1995, raising $54 million from investors. As of January 7, 2017, it was capitalized at $378 billion and had no debt.

[2] Katie Hafner & Matthew Lyon, WHERE WIZARDS STAY UP LATE: THE ORIGINS OF THE INTERNET (Simon & Schuster; 1996).

The 1970s and '80s brought the PC Revolution to homes and businesses. Connections to desktop computers were possible over the telephone system, and subscription services like Compu-Serve and Prodigy were launched. Restrictions on corporate and individual access were eliminated. The Internet became commercial. A new world dawned.

Entrepreneurs seized the moment. By 1995, tens of millions of U.S. users were, without any programming skills, able to log onto the World Wide Web, a handy address system devised at a Swiss research center. In applications, new dial-up services used the existing phone system to allow residential users to "call into" the long-distance data links. America Online (AOL) bundled Internet access with its own unique content, a "walled garden." In 1996, the company distributed some 250 million sign-up disks. By 1999, it served over twenty million U.S. subscribers, becoming the world's largest Internet Service Provider (ISP). And its "walled garden" opened up. AOL's subscribers flocked to websites offered to all comers on the Internet.

A notable facet of U.S. policy during this period was the absence of regulation. New business models arose, worked, or failed – whereupon they were quickly displaced by newer test models. If old restrictions and mandates for common carrier regulation had been applied to this new space, emergent innovations would have been blocked. Only by sharply limiting legacy rules of the 1950s, '60s and '70s could the Internet piggyback on the telephone network in the 1980s and '90s – as a paper by the Federal Communications Commission, The FCC and the Unregulation of the Internet, detailed in 1999.[3] For instance, "voice over Internet" services were initially stymied by both state and federal regulation; only by removing existing rules, taxes and access charges did this important innovation – which brought head-to-head competition to the erstwhile monopoly "Ma Bell" telephone system – come to market.

B. A New Industry is Born

But dial-up was already being displaced, as cable TV operators – unregulated and free to enter the ISP market – used digital capacity on their video distribution grids to begin providing cable modem service – "broadband." Broadband brought higher data speeds, opening new vistas for information services. The disruption brought a response from the (regulated) incumbent telephone companies, which had long promised to introduce advanced data services. The world had waited, as the local exchange technology was slowly developed, haltingly deployed, and inadequately provisioned. But, spurred by cable competitors, phone operators got serious, bringing technologies such as DSL (digital subscriber lines) and fiber-to-the-premises (FTTP, largely associated with Verizon's FiOS) to

[3] "The story of the Commission and its role in the development of the Internet highlight the benefits of the FCC's early deregulatory efforts to facilitate the growth of computer applications offered over the public telecommunications network… [T]he Commission has acted in numerous ways to ensure that this incredible network of networks continued to develop unregulated…" Jason Oxman, *The FCC and the Unregulation of the Internet,* Federal Communications Commission, OPP Working Paper No. 31 (July 1999), at 6.

market. It was these investments encouraged by deregulation in the early-to-mid 2000s that incentivized phone carriers innovate.[4]

The mass-market Internet platform created robust economic opportunity. Digital content – text, voice, pictures, video – could move rapidly, at low cost, from sellers to buyers. In remarkably short order, thousands of innovative websites were conceived, funded, and launched. In the dot.com boom, 1995-2000, waves of C2C, B2C, B2B (consumer to consumer; business to consumer; business to business) initiatives hit the market. Most failed quickly, some did not. Among the former were Pets.com, DrKoop.com, Webvan, theGlobe.com, and eToys. Among the latter were Yahoo!, eBay, Amazon, and Wikipedia.

The economic numbers are staggering. In a 2011 study, the McKinsey Global Institute (MGI) estimated that, while some 3.4 percent of national income (gross domestic product) in developed countries was directly attributable to Internet services, the category was responsible for an estimated 21 percent of economic growth during the previous five-year period.[5] MGI found that individual broadband subscribers might enjoy consumer surplus equal to as much as $272 annually,[6] but the largest gains are distributed widely throughout the economy in the form of productivity gains, lower prices, and improved products. Some three-quarters of the impact is registered in "non-Internet" industries.

C. What Happened and Why?

This cursory review could be supplemented many times over. With the advent of the wireless web, triggered by the introduction of digital mobile networks in the 1990s and padded with additional mobile spectrum allocations in the 2000s, the Internet has evolved into social media, e-health, locational services, and far more. The Internet of Things – the inter-networking of digital machines ("connected devices" and "smart devices"), vehicles, buildings, and other items – embedded with electronics, software, sensors, actuators, and network connectivity that enable the collection and exchange of data – is now linking billions of devices. New worlds are unfolding. The foundational support for such growth remains constant: open markets. Innovators will always be free to dream, but entrepreneurs need to be free to compete.

Allowing new businesses to disrupt established industries is not always the policy preference of a nation's leaders. Losers are another result of the tremendous advances brought about through innovation. And losers often want to reach for regulation. Indeed, a bias for protectionism has virtually always been the first reflex of the government regulator, both in the U.S. and abroad. The

---

[4] Thomas W. Hazlett & Anil Caliskan, *Natural Experiments in Broadband Regulation*, 7 REVIEW OF NETWORK ECONOMICS 460 (Dec. 2008).

[5] Matthieu Pélissié du Rausas, James Manyika, Eric Hazan, Jacques Bughin, Michael Chui & Rémi Said, *Internet matters: The Net's sweeping impact on growth, jobs, and prosperity*, McKinsey Global Institute (May 2011).

[6] The McKinsey estimate was given as 20 Euros per month. The adjustment to dollars is made using the currency exchange rate on Jan. 14, 2017 (1.06 Euros per Dollars) and U.S. inflation from May 2011 to Nov. 2016 (latest Consumer Price Index available).

discussion that follows is a cautionary one; before seizing the impulse to regulate, deeper thought must be given to regulatory failures. But as barriers have given way, vast new sources of ingenuity have been unleashed.

The Internet was not created by the Department of Defense, the National Science Foundation, IBM, Microsoft, or Al Gore. No particular technological breakthrough or any particular plan created what we now celebrate. That there was a design, engineered by a vision, is an example of what has been called the "epiphany myth."[7] In fact, the Internet's rich innovation ecosystem has not been devised by plan, but has evolved through the rigors of competitive enterprise.

It often escapes notice that this magically productive incrementalism is facilitated by open markets. These, in turn, are supported by property rights, the freedom to contract, and a court system for enforcement. Such an environment encourages risk-taking and welcomes rivalry. It foments innovation. These social constructs lead college students to win venture capital from billionaires and virtually force the most powerful people in society to sit quietly and listen attentively to the next big idea. If only they might discover it.

As toasted by Nobel Laureate in Economics, Vernon L. Smith, all this relies on "Humanity's most significant emergent creation: markets."[8]

The right rules can help, while the wrong rules can hurt. And there is no guarantee that what garners political support in any given situation will redound to the benefit of consumers, workers, innovators, and citizens. As Friedrich Hayek observed long before the Internet, "[o]nly if we understand why and how certain kinds of economic controls tend to paralyze the driving forces of a free society, and which kinds of measures are particularly dangerous in this respect, can we hope that social experimentation will not lead us into situations none of us want."[9]

IV. Americans With Disabilities Act

Regulations that live long beyond technology and industry cycles can lead to negative consequences for consumers – in particular, consumers with disabilities. Here the regulatory impulse is forcing website operators to adopt technologies that check a regulatory box but diminish the customer experience.

The Americans with Disabilities Act (ADA) pre-dates the rise of the internet as a significant venue for retail and other activities, and it contains no references to the internet or websites. But, in 2006, Target settled a class action suit that alleged target.com was inaccessible to the blind, and since then the applicability of the ADA to the internet has been frequently litigated in federal courts. Following this settlement, advocacy groups and the plaintiffs' bar have been suing a range of public

[7] Scott Berkun, THE MYTHS OF INNOVATION (O'Reilly Media; 2010).
[8] From his celebratory toast in accepting the Nobel Prize in Economic Science (Stockholm, Dec. 2002), in Vernon L. Smith, DISCOVERY: A MEMOIR (Author House, 2008), at 329.
[9] F.A. Hayek, *The Road to Serfdom*, preface to the 1956 paperback edition.

accommodations – grocery stores or other sales or rental establishments, places of education, restaurants – on the basis that these accommodations' websites are not compliant with the ADA because they are not accessible to people with visual or hearing impairments.

Since the Target decision courts have been divided over whether websites are places of "public accommodation," and there is no guidance as to what level of accessibility is required. At the same time, the Department of Justice (DOJ), which enforces the ADA, says it interprets the ADA as being applicable to websites. In 2016, the DOJ said it will issue guidance in 2018 that would "require public entities and public accommodations that provide products or services to the public through websites on the Internet to make their sites accessible to and usable by individuals with disabilities."

In the absence of clear legislation or judicial precedent, companies and universities are left uncertain as to the appropriate level of accessibility for their internet presence. This uncertainty together with the fear of costly litigation threatens innovation. It is important to note that, were accessibility features cost-free, there would be no issue; websites would simply upgrade, and be happy to do it as they bring their content (and, perhaps, retail sales) to a wider audience.

Alas, there are costs involved. The way in which websites are created and then expanded to provide for wider access involves differential investments. In almost any innovation, limited markets (or product versions) are tested on small audiences first; when demands are revealed and services become established, they spread. This pattern begins with "early adopters" and then flows to the "mass market." When unclear rules drive up the costs of an initial prototype, the innovations of start-ups can be crushed or never get off the drawing board. This is an appalling outcome, particularly for the disabled who benefit disproportionately from advances in digital commerce and data networking.

President George H.W. Bush signed the ADA in 1990. The law has been described as an "equal opportunity" law, similar to the Civil Rights Act, for individuals with disabilities. It prohibits discrimination against people with a physical or mental impairment that substantially limits one or more major life activities, including working, communicating, hearing, seeing, and speaking. More specifically, Title III of the ADA prohibits discrimination by public accommodations, which the law defines to include private entities whose operations affect commerce, and which falls within one of 12 enumerated categories such as retail services and schools. In addition, the ADA and its associated regulations set forth requirements to ensure that people with disabilities are not excluded or otherwise treated differently than others because of the absence of accessible electronic and information technology. Neither the law nor its implementing regulations address the internet.

A number of cases, approximately 244 in the 22-month period January 2015-October 2016, have been filed.[10] One of these involves Winn-Dixie Stores, which have both physical stores and a website that offers services including store coupons for use in stores and the ability to refill prescriptions. In that case, the plaintiff, a blind man, sued Winn-Dixie because its website was not

[10] http://www.adatitleiii.com/wp-content/uploads/sites/121/2016/10/Number.jpg.

accessible through the use of screen reader technology or any other technology provided on the Winn-Dixie website. Winn-Dixie responded by arguing that it is under no obligation to ensure website access, asserting that the ADA only applies to physical locations. The DOJ disagreed, filing a Statement of Interest in the case asking for the court "to clarify public accommodations' longstanding obligation to ensure that individuals with disabilities are not excluded, denied services, or treated differently than other individuals because of the absence of auxiliary aids and services, such as accessible electronic technology."

To date the DOJ has not issued any guidance that would allow entities to determine whether their website meets ADA standards. Likewise, Congress has not addressed the absence of clarity around the ADA's applicability to websites. Legislation could clarify that the ADA does not apply to websites or that the ADA does apply with compliance obligations defined. Until then, industry groups (Chamber of Commerce, etc.) are left to challenge ongoing litigation and/or develop best practices for accessible websites, which may shield some of the litigation risk. Regardless, the uncertain regulatory framework chills innovation.

A rather sensational case has recently illustrated the costs of ambiguity. The University of California, Berkeley has posted class lectures for a wide variety of its courses. These online learning videos have become extremely popular as educational tools. They involve a simple reformatting – capturing a professor's in-class performance, and then linking the program through the UCB website without any significant post-production investment. Cheaply made, over 40,000 hours of instruction was available, and created MOOCs – massively open online classes – that students around the world have taken to learn and for college credit.

But they do not all provide closed captioning, and can thus be difficult for deaf viewers to follow. Some present graphs in just one color, not well suited for the color blind. Two deaf students complained to the DOJ, and the DOJ filed an ADA complaint against Berkeley. The University has responded by taking down its 20,000 educational videos from YouTube. The immediate impact was to diminish learning opportunities – for abled and disabled, alike.[11]

V. The Sharing Economy

One perfect example of how regulations can stifle innovation arises from the increased impulse to regulate the sharing economy – that is the new marketing methodology powered by network connectivity that allows providers with excess capacity to directly connect with consumers who wish to take advantage of the capacity. Examples of the new economy abound and are no doubt familiar – Uber, Lyft, Gett, and Juno provide transportation services that compete with traditional taxi systems; Airbnb provides lodging services in competition with traditional hotels and motels; Zipcar competes with car rental companies; Kickstarter's loan system competes with traditional banking and financial organizations; and so on.

[11] Andrew Ferguson, *Berkeley Goes Offline*, THE WEEKLY STANDARD (March 20, 2017).

There are, manifestly, immense advantages to this new form of commerce. Providers get to sell, in effect, partial shares of ownership or use in their goods. Consumers, likewise, can have on-demand provisioning for their needs so that they can avoid capital expenses and long-term ownership costs while retaining the convenience of usability. The net economic benefit to the new providers and users is undoubtedly positive for both.

The economic losers in the equation are the old-line traditional providers whose business model is disrupted by the change. Yellow cab taxi medallions in New York City (once) conveyed an exclusive right to supply car transportation. As a result, those few medallions that existed were sold for sums exceeding one million dollars. No more. Ride sharing apps have crushed that monopoly.

The entrenched industries cannot, of course, resist change by publicly arguing that "it is bad for our business." Instead, they do what rent-seekers[12] do – promoting more subtle strategies to enact regulations that erect barriers to competition. These have the effect of favoring their existing business models. Sometimes these laws are erected in the name of "security" and sometimes the watchword is "safety" or "privacy." But whatever their facial justification, in many instances the advanced regulatory agenda is only nominally tied to the result.

Resistance to Uber and Lyft provides a perfectly good example.[13] The sharing economy is one of flexibility. Uber and Lyft depend heavily on part-time drivers that have other jobs, and rotate between assignments as circumstances permit. Uber and Lyft gain and lose drivers at rates that traditional businesses could not withstand. But this fluid situation not only assists drivers seeking flexible hours, but drives competition increasing welfare. UberX ride sharing has been associated with as much as $6.8 billion a year in gains for riders,[14] and has been shown to increase customer satisfaction with traditional taxis – forced by enhanced competition to increase the quality or their performance.[15]

And so, when entrenched transportation interests felt threatened by the Uber and Lyft model they advanced time-consuming safety regulations as their objection. In Maryland, for example, traditional taxi companies first opposed a new regulatory system for Uber and Lyft on the ground that it provided an inadequate background check of Uber and Lyft drivers – arguing that one requiring weeks of checking was more appropriate. Happily for Maryland's consumers, the legislature eventually adopted a proposal that offers more streamlined background checks.[16]

Consumers in Austin were not so lucky. Austin rejected a similar streamlining proposal and insisted that Uber and Lyft drivers go through the same cumbersome fingerprinting and background checks

---

[12] Rent-seeking is when an entity or individual seeks a benefit from the government to obtain a favored status.

[13] Resistance to bad behavior at Uber is warranted. Allegations of CEO immaturity, regular sexual harassment of employees, and use of software to deceive regulators should be taken seriously, and if true, remedied.

[14] Peter Cohen, Robert Hahn, Jonathan Hall, Steven Levitt & Robert Metcalfe, *Using Big Data to Estimate Consumer Surplus: The Case of Uber*, NBER Working Paper No. 22627 (Sept. 2016).

[15] Scott Wallsten, *Has Uber Forced Taxi Drivers to Step Up Their Game?* THE ATLANTIC (July 9, 2015).

[16] https://www.washingtonpost.com/news/dr-gridlock/wp/2015/04/14/maryland-lawmakers-approve-uber-bill-send-it-to-hogan-for-signing-into-law/?utm_term=.36b2d97022d1.

that traditional taxi drivers did – a requirement that, given turnover at Uber and Lyft, was impossible for the new flexible economy to meet. As a result, Uber and Lyft both left Austin – leaving consumers the use of traditional transportation methods instead.[17] In early June 2017, Uber and Lyft returned to Austin.[18] The re-entry occurred due to state legislation, adopted in 41 other states, that overturns the local rules creating barriers (like the mandate to fingerprint drivers) demonstrating a potential way in which competitive solutions can be brought to the market.

These two vignettes are just the tip of the regulatory iceberg. An anecdotal survey suggests that some form of regulatory restriction is being considered in more than a dozen states. Some of the regulations may prove beneficial, but a number of them seem to be little more than an effort to interpose governmental restrictions to protect existing businesses, firms that have often been significant financial contributors to local office holders.

This iron-triangle of business-contribution-politician helps business actors engage in "rent-seeking," profiting by imposing costs on others. The rent, in this case, is created by the higher prices for transportation that (regulated) consumers will pay, parts of which go to the traditional transportation services and other portions of which wind up enabling their political protectors.

The ride sharing market experience is not unique. A similar dynamic is playing out, for example in New York's efforts to regulate how its private citizens rent out their own homes on Airbnb.[19] As with competitive barriers in transportation services, new limits punish consumer and the small-scale, part-time suppliers, while benefits are enjoyed by large, incumbent hotel chains. In the age of the Internet-enabled economy, crony regulations from a by-gone era that challenge innovation merit careful reevaluation; security and privacy interests can be met through alternative means reserving regulation for the most critical of human and technology interdependencies. And rules should always be subject to realistic cost-benefit evaluation.

VI. Cybersecurity and the Wassenaar Export Controls

While Uber and Lyft battle regulations at the local and state levels, the cybersecurity industry is being stymied at the federal and international levels.

These innovative companies are up against some tough competition. Not just other American cybersecurity companies, but also Russian intelligence agencies, the Chinese security state, and some of the richest and smartest members of organized crime that Eastern Europe has produced. Even worse, they now are being hamstrung by Western governments that want to make it harder for them to sell their products abroad. Through something known as the Wassenaar Arrangement the governments want to classify basic cybersecurity tools as "weapons" and make them subject to export controls. That regulatory response is a mistake.

---

[17] https://www.nytimes.com/2016/05/12/opinion/how-austin-beat-uber.html.
[18] https://www.texastribune.org/2017/05/29/texas-gov-greg-abbott-signs-measure-creating-statewide-regulations-rid/.
[19] https://www.nytimes.com/2016/10/22/technology/new-york-passes-law-airbnb.html.

Consider how cybersecurity companies operate: Once a new attack has been identified, they work to understand exactly how it functions. They collect hacker tools and use those tools to attack their own networks and their customers' networks to see what vulnerabilities need to be shored up. They trade information with a global network of "gray hat" hackers intrigued by the intellectual challenge of finding and exploiting flaws. They may offer bounties to hackers who identify and help them fix security flaws before the black hat hackers can exploit them. Since the flaws are almost always unanticipated problems with existing software like Windows or Office or iOS, the fix usually requires a patch to change the way existing software operates, or to add functionality that the writers of the existing software didn't expect to need. It is a fast-paced race against time and against adversaries, a race we all want the industry to win as often as possible.

All of these security tools are dual-use. Just as "good guys" can use the technology to protect us (by, say, testing their own networks), authoritarian governments can exploit the same new technology for malicious reasons. Evil empires can use these tools to hack their own citizens' phones and computers, intercept their communications, and harass civil society advocates in order to keep their hold on power. As surveillance technology has become popular with authoritarian governments, policy makers in the West reacted by adopting laws to prevent Western companies from exporting cybersecurity tools without a license.

The origins of the policy may be straightforward, but its impacts can be perverse. Western governments, including parts of the U.S. government, have begun advancing a regulatory regime that will slow industry down, preventing it from testing customer networks, and scaring off the researchers and gray hat hackers on which it depends. As with most ideas for regulation, the governments advocating controls on cybersecurity tools have identified a real problem that they want to solve. But they have chosen a regulatory solution because it feels familiar, not because it will actually work. It is a classic example of the bureaucratic memo made famous by "Yes, Minister": "Sir, we must do something about the problem. This regulation is something. Therefore, we must do this." The chosen vehicle is the Wassenaar Arrangement.

Export controls have a long history among Western countries. We used controls on technology and weapons to keep the benefits of Western research from reaching the Soviet bloc during the Cold War. After that, we kept the controls as a way of sanctioning rogue states like North Korea. To the countries that wanted to keep surveillance tools away from the worst governments, the idea of treating those tools like weapons had a lot of appeal. With partial support from the United States, European members of Wassenaar agreed that all countries should impose controls on exports of "intrusion software." The U.S. Commerce Department then began a rulemaking process to impose these controls on American industry.

This is a disaster for the cybersecurity industry. To take a simple example, think of the companies that do "penetration testing" on corporate networks using tools already in use by hackers around the world. These tools are "intrusion software" by any definition. They are also essential to protecting corporate networks around the world. If a license is needed to carry such tools out of the country,

or to add new components to tools as new hacker tactics are discovered, an industry that today updates its software on a daily or even hourly basis will be stuck waiting for licenses that are granted at the speed of government. We'll all suffer if that happens.

More importantly, the proposal overlooks one crucial fact about the malicious code at the heart of penetration tools. It is not Western technology developed by Western companies, like cruise missiles or supercomputers. Itis crimeware, developed and used first by criminals. And no criminal will ask for an export license before selling those tools to any willing customer. Since authoritarian regimes can buy the tools on the criminal black market – or from countries that are not part of international control agreements (China, for example) – all the licensing in the world won't keep these tools out of their hands. The regulations just slow the cybersecurity industry to a crawl without seriously inconveniencing authoritarian governments.

It gets worse. The actual definition of "intrusion software" in this international regulation is remarkably broad. It covers any software that "avoids detection by monitoring tools" or "defeats protective countermeasures" to modify the standard execution path of a program. Those certainly sound like sinister activities, but as a practical matter, any program that adds features or patches holes in a commercial software program has to defeat countermeasures and modify the operation of the faulty software. Practically any new cybersecurity software does that. Also proscribed are tools that extract information from computers after defeating countermeasures in standard software. Again, any new technology will defeat the countermeasures of existing software, and extracting information from systems that weren't built to provide it is one of the most common and promising security measures now available; it allows security managers to spot machines that have been taken over by hackers and are acting in anomalous ways.

What this boils down to is that most cybersecurity tools are likely to fall into the new regulation and to require licenses. Sure, they will probably get those licenses eventually, but the lags can be deadly. In the wait times, security will get worse. We will fall further behind in the arms race with hackers. And, for the reasons already noted, these misguided regulations will not keep authoritarian governments from spying on their own people or attacking networks around the globe.

Export controls on intrusion software were meant to address a real problem. But even the U.S. human rights groups that commented on the proposed rule said that they would not work and should be reconsidered. The Commerce Department has withdrawn its original proposal, and it is trying to decide what if any new rule it should write. The best thing it could do right now is nothing – no new rule on intrusion software.

In short, there have been active efforts to create a new regime that would cripple one of the success stories for the United States in the internet economy. The restrictions would harm a new and growing industry without achieving any of the goals the regulators are aiming at. There's nothing wrong with the asserted goals, but the impulse to regulate in a way that places rigid and counter-productive rules in the center of a fast-moving industry is deeply unwise.

VII. FTC Consent Decrees

Among the alphabet-soup of agencies that make up the bulk of the federal government, the Federal Trade Commission ("FTC") is unique. Some agencies have authority to enforce specific statutes that directly affect almost everyone in the country, and others have statutorily-delegated broad authority to regulate the conduct of a narrow group of firms or individuals. In the former case, the authority is narrow but the scope is broad, in the latter case the authority is broad but the scope is narrow. The FTC is one of a small number of agencies whose authority is broad and the scope of whose authority is also broad.

Agencies that have such power are subject to important checks on how they use that power. But over the past two decades the FTC began exercising broad authority without triggering judicial review. Rather than use standard tools, the FTC now threatens to sue firms to force out-of-court settlements. Firms are likely to prefer to settle such actions (in so-called consent decrees) to spending years in costly and burdensome litigation. But there are external costs. Once having procured a given settlement, the FTC then turns around and enforces those terms and concessions against others who were not party to the original action. Yet, the terms being enforced were obtained without the traditional assurances of judicial review. Over the past twenty years, the FTC has used this strategy literally hundreds of times.

One hundred years ago, Congress gave the FTC broad powers specifically so that it would be able to keep up with rapidly changing industries. Of course, the pace of change in modern technology allows businesses to now develop faster than ever before. The FTC, with its flexible statute, isn't constrained by the slow and deliberative pace of administrative law as practiced in other regulatory agencies. Hence, the FTC has intervened in hundreds of cases involving technology firms, from disputes involving privacy and security and potentially monopolistic practices. The firms investigated include Google, Microsoft, Facebook, Snapchat, and Twitter.

The FTC

The Act that established the FTC in 1914 gives it the authority to proscribe and take action against "unfair methods of competition" and "unfair and deceptive acts and practice" that affect interstate commerce. At its broadest, the agency can take legal action against any company in the United States (no matter how large or small) engaging in any practice that three of its five commissioners feel is "unfair."

"Unfair" is ambiguous. In the 1970s, the FTC attempted to ban all advertising directed to children as unscrupulous. This led to a public and political backlash against the FTC as a "national nanny." Today, for a practice to be unfair, it must have a substantial negative effect on consumers that is not offset by other more substantial benefits, and it must be unavoidable by consumers.

Of course, high-tech firms should not be able to avoid the reach of the law simply because they move quickly. But, in its eagerness to make use of its authority – for good or for ill – the FTC has jeopardized basic legal principles.

Federal agencies exercise their powers in one of two ways: making rules or enforcing statutes (which may require rules made pursuant to the legislation). In the former case, they are acting like mini-legislatures, gathering evidence and deliberating about what rules are best before formally imposing them. In the latter case, they are acting like courts, investigating potential wrong-doing, giving each side opportunities to present evidence, and ultimately issuing an adjudicatory opinion. In both cases, whatever the agency does can be challenged in court. It is the role of the federal judiciary to ensure that federal agencies follow the law.

But, the FTC almost never goes to court. The FTC relies on consent decrees. It threatens to take legal action against firms on "unfairness" grounds, unless those firms agree to settle. The process of challenging the FTC takes years, often costs millions, and – even for parties that ultimately prevail – results in substantial harms. Reputations, money, and executive time are all squandered. Indeed, one of the only cases in which a firm has refused to enter a consent decree has been ongoing for more than half a decade and has already put the targeted company – one of two medical testing laboratories in the country that specialized in cancer detection – out of business. Perhaps this was the efficient result, but perhaps it was just an unfortunate outcome. No court will decide, and justice will be imposed by circumstance, not law.

The advantages to the FTC of this approach are obvious. It effectively never loses a case. It can trumpet its hundreds of consent decrees as wins before Congress and the public. And it can use these consent decrees to legitimize its preferred policies and enforce them against future companies, all of this without the fuss and muss of adjudications that may ultimately be overturned by courts. By ignoring important safeguards, regulators may be undermining important legal protections without offsetting benefits to consumers.

Perhaps the most concerning aspect of the FTC's efforts is how aggressive it has been in pursuing them. This is best seen in the design of its consent decrees: its standard demand is that companies agree to 20 years of ongoing outside audits and oversight by the FTC. This is a remarkable demand for an agency whose efforts have largely focused on regulating technology firms and other firms' use of technology. Twenty years ago, most people connected to the Internet by dial-up modems, using services like America Online.

As captured by long-time federal judge Douglas Ginsburg, "The 20-year term seems to be almost certainly inappropriate in high-tech industries with very fast turnover in product design. … How many iPhones will there be in 20 years? Twenty years of supervision over that kind of evolution strikes me as completely unfounded." Consider Myspace: in 2007 it was the dominant social media platform, valued at $12 billion, but by 2011 it had been almost entirely displaced by Facebook and was sold for a mere $35 million. Despite its rapid fall from relevance and unlikely future, in 2012 the FTC brought an enforcement action against Myspace and forced the company into the same 20 year consent decree as it imposes upon any other company.

This concern is compounded by the FTC's frequent refusal to adopt official guidance that would alert businesses to the sort of conduct that the agency considers unfair. As Judge William Duffey, a

judge involved in one of the only two cases that have gone to court challenging the FTC's consent decrees, said, "how does any company in the United States operate when [it asks the FTC] 'tell me exactly what we are supposed to do,' and you say, 'well, all we can say is you are not supposed to do what you did.' … [Y]ou ought to give them some guidance as to what you do and do not expect, what is or is not required. You are a regulatory agency. I suspect you can do that."

The FTC's response to these concerns is that it is doing precisely what Congress created it to do: using its broad, flexible, authority to address concerns that arise in rapidly-moving industries. Technology is changing so fast, the argument goes, that it would be impossible for the agency to issue more formal guidance. The problem is with this is that the FTC is charting a legal course that is at odds with that being charted by the courts – to which agencies like the FTC are intended to be accountable and subservient.

This is best seen in the nearly 200 cases the FTC has brought relating to privacy and data security. These are important and difficult legal issues. Surely, privacy and security are important to consumers and business alike. In an important recent case, the Supreme Court reaffirmed a basic legal principle: that legal action needs to be predicated on concrete harm. We do not want the power of the state to be invoked against citizens based on merely hypothetical or speculative claims of "harm." Compare this to the FTC's data security cases, where the agency has argued that a company's security practices that may have allowed hackers to obtain customer information that may have been subsequently used by those hackers in way that may have been harmful to some consumers is sufficient to justify action by the FTC – even where there is no evidence, after nearly a decade of investigation of a breach, that any compromised data was used, or that any consumers were harmed. In a recent judicial opinion – involving the only case in which a company has gone to court to challenge the merits of the FTC's data security cases – three federal judges agreed, reading words like "'probable' and 'reasonably expected,' to require a higher threshold than that set by the FTC. In other words, "we do not read the word 'likely' to include something that has a low likelihood. We do not believe an interpretation that does this is reasonable."

The FTC has put together a playbook that allows it to sidestep most of these concerns. By relying on consent decrees, the FTC need not worry about judicial review of most of its actions. Over the course of several years, it can build up a body of consent decrees that it can then point to as establishing binding legal norms. This is precisely what it has done with its privacy and data security cases. This behavior enables the FTC to operate wholly outside of the law.

The practice is contagious. In recent years, both the Federal Communications Commission ("FCC") and the Securities and Exchange Commission ("SEC") have increasingly embraced the FTC's playbook. After a series of high-profile losses in federal court last decade, the SEC began relying more heavily on internal adjudications and consent decrees to enforce its authority. And the FCC has also followed in this path, beefing up its enforcement resources in recent years and relying on aggressive consent decrees to develop policy.

Agency leaders are earnest in their efforts. Dedicated public servants will try to use their agencies' authority to do good in the world. But cross-checks are vital. Guidance by Congress, judicial review by the courts, and legal protections for those subject to regulation are key elements of the regulatory loop. They are not mere legal formalities. They ensure that agencies act reasonably and wisely, in ways that consider a wide range of factors and that do not conflict with other policies. These formalities also ensure that those subject to the agency's authority are provided notice of what conduct is and is not prohibited.

The concerns about the FTC are based in fact, as the story that follows illustrates.

A. Taking the Consent out of Consent Decrees

Nobody fights an FTC consent decree. At least no one did until Mike Daugherty came along.

In May 2008, Daugherty was the CEO of LabMD, a cancer testing lab. That month, he was called by a security researcher he'd never heard of. The researcher claimed that a lot of LabMD's patient records were available on the internet, courtesy of a music file-sharing program similar to Napster. The security researcher wanted to be paid to help LabMD clear up the security breach, warning that if Daugherty didn't retain these services he would need to be reported to the FTC.

That sounded like extortion to Daugherty, who refused. Before he knew it, the researcher had provided its work to the FTC, which opened an investigation. Asked what he had done wrong, the FTC told him that poor security was an "unfair" business practice, even though he was compliant to the government's security standards for health care providers, even though the FTC had never publicized any guidance suggested his firm's security standards were problematic, even though his company was the victim of the security breach, and even though there was no evidence that any of Daugherty's patients had been harmed by the breach. After painful and extensive demands for Daugherty's records, the FTC told him that the only way to avoid a lengthy trial was a consent decree regulating LabMD's security practices.

Daugherty was convinced that he hadn't done anything wrong, that the records had not actually been taken from his network, and that the FTC was turning a private protection racket into a government-sponsored protection scheme.

He decided to fight. Nearly a decade after that first call, the risk that employees will install file-sharing software on corporate networks seems like a quaint bit of computer security trivia. But Daugherty is still fighting, and so is the FTC. At one point, Daugherty persuaded the FTC's own administrative law judge to drop the case, but the Commission reinstated it. Meanwhile, the years of legal skirmishing have taken their toll. LabMD is out of business, its servers stacked in Daugherty's garage, a security solution even more drastic than the FTC demanded.

But the FTC is not satisfied. It will not stop litigating until the broken company signs on the dotted line. Daugherty says the FTC is staffed by "professional bullies." But the FTC is making a point – a point it doesn't want any company in America to miss:

Nobody fights an FTC consent decree.

VIII. Internet of Things

Like the sharing economy, the last ten years have seen a vast expansion in the growth of the Internet of Things (IoT). According to Gartner,[20] the base of IoT units installed on the network will expand from fewer than 1 billion in 2009 to more than 26 billion by 2020. Perhaps more impressively, by that time the number of IoT units will exceed the number of non-IoT connected equipment, such as laptops, and personal phones – by a margin of almost 400%. It is fair to say that IoT growth is ***the*** wave of the future – whether we like it or not.

There are many reasons for this growth. To begin with the most obvious, connectivity enables collaboration and communication. An IoT enabled car can be a driverless one, eventually. An IoT thermostat can reduce heating and cooling costs. An IoT alarm system lets you permit the workman to enter even when you aren't present. Perhaps even more saliently, the costs are miniscule – indeed, the reasons for the increase in IoT often have little to do with the utility of connecting to the network. The costs of building in connectivity are so small that it almost makes no sense from an economic perspective to construct a new product without connectivity these days.

This rush of innovation and expansion is, however, at risk – both from the malicious actors and, paradoxically, from the government. The malicious risk is evident – the recent Mirai botnet hijacked routers and other IoT systems and made them slaves to a malicious actor who used their combined power to launch denial of service attacks on individuals, companies, and even an entire country (Liberia). To some degree the absence of security in IoT devices makes them a risk.

But an equal risk (if not a greater one) arises from the possibility of government regulation – the type of regulation that can stifle innovation without being effective (e.g. the risks to the cybersecurity industry described in Section V.). Most notably, government risks looking at the insecurity of the IoT as a reason to regulate these devices that span sectors. That would be dangerous.

The rationale for regulation is that security is a private good but has external effects on other actors. These externalities can be negative or positive. By securing my own server or laptop against intrusion, for example, I benefit others on the network since my computer cannot be hijacked, say, into a botnet and used to attack other people. I also lessen returns available to malicious hackers, and so tend to reduce their presence. Indeed, almost every positive measure improves the overall level of cybersecurity by raising the costs of attack.[21]

---

[20] http://www.gartner.com/newsroom/id/2636073.

[21] *See* Christopher J. Coyne, *Who's to Protect Cyberspace?*, 1 J.L. Econ. & Pol'y 473, 475-76 (2005).

But cybersecurity also has negative external effects, in two ways. The first is a diversion effect: Methods of protection, such as firewalls, have the effect of diverting attacks from one target to another, making improvements in one actor's security is equivalent to a decrease in security for systems that are not as well-protected (even though that owner has not sought to increase his or her own vulnerability).[22] Some have argued that the second negative effect is a pricing problem that reflects the failure of the private market. Sometimes, the price of a product doesn't have all of the costs of the product built in. When costs like that aren't included in the price of a product, the product is too cheap and somebody else winds up paying the costs in the end. Total costs will be higher than in a more efficient system.

Whether the market has failed in the IoT security arena is a topic of some debate, and this paper is not declaring which argument wins. Rather, the argument illustrates the point that in certain circumstances – cybersecurity may be one – industry phenomena can have both positive and negative external effects that can be confusing and pose a significant policy challenge. Either circumstance suggests a role for government. But identifying which factor predominates is essential, since the characterization will point in differing policy directions. Private goods that cause positive externalities are typically encouraged and perhaps subsidized (e.g. the beneficial tax treatment of charitable giving). Not enough of the good exists and we want to encourage investment. By contrast, private goods that cause negative externalities are taxed, regulated, or subjected to a liability regime (e.g. sale of tobacco products). We want less of the good or we want the producers to internalize the external costs and reduce the level of production to one commensurate with its true costs.

But there are at least two reasons to be skeptical of the government's engagement in the private sector's provision of cybersecurity in the IoT. First, there are good reasons to doubt the ability of the government to systematically make the right choices. In a perfect world, the "right" answer would be obvious. But in the real world, experts disagree; lobbying and political influence often define the answer. We have good reason to be concerned that the subsidies, taxes, and regulations enacted will not foster the efficient result, as with, for example, the ethanol subsidies that have been around for years even though it is commonly known they are not a good investment, harming consumers and hurting the world's poor. This concern is not unique to the cyber arena.

Second, the pace of IoT transformation is extremely rapid while government makes policy through slow moving, hierarchical decision-making structures. It takes years or decades for laws and regulations to be implemented, by which time they are often out of date. As one expert, put it: "The attackers are two years ahead of the defenders, security vendors, who are two years ahead of market, which is two years ahead of compliance, and legislation is five years behind that. … [Legislatively

[22] Bruce H. Kobayashi, "Private Versus Social Incentives in Cybersecurity: Law and Economics," in *The Law and Economics of Cybersecurity* (Mark F. Grady & Francesco Parisi eds., Cambridge University Press 2006), at 16. Less persuasively, Neal Katyal has argued that purchases of private security goods spread fear, thereby potentially increasing the crime rate. *See* Neal K. Katyal, "The Dark Side of Private Ordering: The Network/Community Harm of Crime," in *The Law and Economics of Cybersecurity*, at 202.

mandated cyber security] practices may be even more stale once enacted. It's unlikely the law could ever keep pace, given the glacial pace of legislation."[23]

Worse, regulations are "sticky." Once adopted they are difficult to change, modify, or eliminate (e.g. the ADA example in Section III). In the non-cyber/non-IoT realm, the price of stickiness is real but more manageable, given the pace of change. Outdated regulations about postal rules have no real effect in a world where the postal service itself is almost obsolete. But, again, in a dynamic world like IoT, even if the regulation is reasonable when proposed, it becomes systematically unreasonable soon thereafter. A perfect example of this phenomenon is the 8-10 year journey it took to develop federal cybersecurity information sharing legislation – by which time the utility of information sharing had appreciably diminished in light of changing threat streams.

Markets need information to function. Until recently, information about threats and vulnerabilities was inadequately conveyed in the cyberspace market. Certain policy measures might help firms, individuals, and institutions to learn more quickly about security issues as they emerge. But regulations might also hinder that, creating the very "market failures" that they were intended to avoid. We ought to tread carefully. New rules, particularly in the IoT space, should be narrowly targeted, and positive incentives preferred over broad market restrictions. And cost-benefit scrutiny should be applied early and often.

Externalities exist in the IoT, yet deep skepticism about government authority is warranted. Put bluntly, by the time a notice and comment rulemaking has taken place, the technology at issue will likely have been made obsolete. Indeed, in the time it typically takes to write a Federal rule, under Moore's law the average speed of computer processors doubles – the law is chasing technology and can never catch up. Rules that enable decentralized, competing actors to make socially useful contributions to cybersecurity form the path to optimal public policy.

IX. Conclusion

Every regulation is adopted to solve a problem, so every regulation, on its face, seems like a good idea. Unfortunately, every regulation also carries two risks: that it will not be an effective solution to the problem it is intended to solve, and that it will create additional problems. These risks are particularly acute in high-tech fields, where technology, markets, norms – where everything that defines whatever we may be trying to regulate – are exceptionally complex and changing faster than any regulation possibly could. The result is that regulations are particularly unlikely to effectively solve problems but they are particularly likely to cause other unintended consequences.

This theme has been seen throughout this paper. Attempting to port the laudable goals of the Americans with Disabilities Act to the Internet, to ensure that disabled Americans are able to benefit

[23] *"White House Cybersecurity Plan Feared Inadequate By Experts, Could Violate Privacy,"* E-Commerce Alert (May 17, 2011) (quoting Josh Corman, Research Director, 451 Group), http://www.e-commercealert.com/article1067.shtml.

from the volumes of information online, has resulted in massive amounts of information being removed from the Internet – yielding no benefit and creating substantial harm. Regulations purporting to protect consumers from some of the legitimate concerns raised by sharing-economy services are often advanced by old-economy firms seeking to protect less efficient business models and, as a result, may end up denying consumers the benefits of sharing-economy services while doing little to actually mitigate any actual harms that may come from these services. Attempts to regulate the distribution of cybersecurity tools, in order to prevent them from being used for nefarious purposes, has little effect on the bad guys (who don't care about these regulations) but does slow down the good guys (who depend on these tools to improve the security of computer systems and to protect them from attack).

The discussions of the FTC's attempts to regulate firms' privacy and security practices using consent decrees in Part VI and the regulatory challenges created by the Internet of Things in Part VII provide cautionary tales about the dangers of regulation in high-tech industries. In order to keep pace with technological change, the FTC has foregone basic principles of sound law, abandoning the very semblance of due process as it forces firms into 20-year consent decrees and then uses those consent decrees to bootstrap enforcement actions against other firms. The FTC's plight is understandable: it is trying to regulate an industry moving faster than the law can operate. But its solution – to abandon the very principles that give law its legitimacy – is unsound. The Internet of Things is a case study of a problem that in many ways appears to need regulation, but where it is unclear what regulation could actually do to improve upon the miserable status quo. No matter how miserable that status quo may be, the lesson is stark: first, do no harm. The impulse to regulate is never, itself, either a justification for or guide to regulation; if we let it be either, regulation itself can easily be the first step toward making things worse.

The evidence adduced above suggests a common theme – regulatory action by the Federal government is often well-intentioned, but in many circumstances it imposes costs on consumers that are greater than the benefits offered. This is particularly true in the dynamic and innovative technology space where the dead weight of a federal regulatory hand routinely stifles or threatens to stifle new technologies in favor of entrenched systems of economic order. The evidence seems to clearly suggest that, at a minimum, a regulatory response should be adopted only after other possible responses have proven unavailing and that the regulators should approach their task with a heightened sense of humility about the validity of their judgments.

We therefore propose a set of questions that can facilitate evaluation of an issue to assess whether regulatory measures are appropriate in light of the challenge and foreseeable results should the government elect to continue or impose new regulations.

1. How significantly will the technology or trend I am trying to regulate change in 12, 24, or 36 months?

2. Do arguments for greater regulation based on fairness, security, or safety have a sound evidentiary basis?

3. Is the risk of waiting to regulate outweighed by the risk of acting now?

4. Is the proposed regulation the narrowest and least invasive way to address the primary problem? If not, what should I adjust?

5. Is the regulation sufficiently clear and written in plain English such that a reasonably intelligent commercial actor can remain compliant?

The future will be more connected, not less, which means the ripple effects of bad regulations will be amplified. It is imperative that regulators tread lightly.