# Permissionless Innovation

# Permissionless Innovation

## The Continuing Case for Comprehensive Technological Freedom

ADAM THIERER

MERCATUS CENTER
George Mason University

The Mercatus Center at George Mason University is the world's premier university source for market-oriented ideas—bridging the gap between academic ideas and real-world problems.

A university-based research center, Mercatus advances knowledge about how markets work to improve people's lives by training graduate students, conducting research, and applying economics to offer solutions to society's most pressing problems.

Our mission is to generate knowledge and understanding of the institutions that affect the freedom to prosper and to find sustainable solutions that overcome the barriers preventing individuals from living free, prosperous, and peaceful lives.

Founded in 1980, the Mercatus Center is located on George Mason University's Arlington campus.

www.mercatus.org



Mercatus Center at George Mason University
3434 Washington Boulevard, 4th Floor
Arlington, VA 22201
mercatus.org

**Library of Congress Cataloging-in-Publication Data**

Thierer, Adam D.
Permissionless innovation : the continuing case for comprehensive technological freedom / Adam Thierer.
pages cm
ISBN 978-0-9892193-4-1 (pbk.) -- ISBN 978-0-9892193-5-8 (e-book (Kindle))
1. Technology and state. 2. Research--Government policy.
3. Freedom of information. 4. Technology and law. I. Title.
T14.T443 2014
338.9'26--dc23

2014003863

# CONTENTS

*What matters is the successful striving for what at each moment seems unattainable. It is not the fruits of past success but the living in and for the future in which human intelligence proves itself.*

— F. A. Hayek, *The Constitution of Liberty* (1960)

# PREFACE

The central fault line in technology policy debates today can be thought of as "the permission question." The permission question asks: *Must the creators of new technologies seek the blessing of public officials before they develop and deploy their innovations?* How that question is answered depends on the disposition one adopts toward new inventions. Two conflicting attitudes are evident.

One disposition is known as the "precautionary principle." Generally speaking, it refers to the belief that new innovations should be curtailed or disallowed until their developers can prove that they will not cause any harms to individuals, groups, specific entities, cultural norms, or various existing laws, norms, or traditions.

The other vision can be labeled "permissionless innovation." It refers to the notion that experimentation with new technologies and business models should generally be permitted by default. Unless a compelling case can be made that a new invention will bring serious harm to society, innovation should be allowed to continue unabated and problems, if they develop at all, can be addressed later.

In this book, I will show how precautionary principle thinking is increasingly creeping into modern information technology policy discussions, explain how that is dangerous and must be rejected, and argue that policymakers should instead unapologetically embrace and defend the permissionless innovation vision—not just for the Internet but also for all new classes of networked technologies and platforms.

My argument in favor of permissionless innovation can be summarized as follows:

- *If public policy is guided at every turn by fear of hypothetical worst-case scenarios and the precautionary mindset, then innovation becomes less likely.* Social learning and economic opportunities become far less likely under a policy regime guided by precautionary principle regulatory schemes. In practical terms, it means fewer services, lower quality goods, higher prices, diminished economic growth, and a decline in the overall standard of living. Put simply, living in constant fear of worst-case scenarios—and premising public policy upon them—means that best-case scenarios will never come about. When public policy is shaped by precautionary principle reasoning, it poses a serious threat to technological progress, economic entrepreneurialism, social adaptation, and long-run prosperity.
- *Wisdom is born of experience, including experiences that involve risk and the possibility of occasional mistakes and failures.* Patience and a general openness to permissionless innovation represent the wise disposition toward new technologies not only because it provides breathing space for future entrepreneurialism and invention, but also because it provides an opportunity to see how societal attitudes toward new technologies evolve. More often than not, citizens have found ways to adapt to technological change by employing a variety of coping mechanisms, new norms, or creative fixes.
- *Not every wise ethical principle, social norm, or industry best practice automatically makes wise public policy prescriptions.* If we hope to preserve a free and open society, we must not convert every ethical directive or societal norm—no matter how sensible—into a legal directive. Attempting to do so means the scope of human freedom and innovation will shrink precipitously.

- *The best solutions to complex social problems are almost always organic and "bottom-up" in nature.* Education and empowerment, social pressure, societal norms, voluntary self-regulation, and targeted enforcement of existing legal norms (especially through the common law) are almost always superior to "top-down," command-and-control regulatory edicts and bureaucratic schemes of a "Mother, May I" (i.e., permissioned) nature.
- *For the preceding reasons,* **when it comes to technology policy, permissionless innovation should, as a general rule, trump precautionary principle thinking**. To the maximum extent possible, the default position toward new forms of technological innovation should be "innovation allowed." The burden of proof rests on those who favor precautionary regulation to explain why ongoing experimentation with new ways of doing things should be prevented preemptively.

We are today witnessing the clash of these conflicting worldviews in a fairly vivid way in many current debates not just about the Internet and information technology policy, but about other emerging technologies and developments.

Over the past year, for example, taxicab commissions across the nation have tried to stop Uber, Lyft, and Hailo from offering better transportation options to consumers.[1] Similarly, the state of New York has threatened the home rental company Airbnb, demanding data from all users who have rented out their apartments or homes in New York City.[2] Meanwhile, the Food and Drug Administration recently ordered 23andMe to stop marketing its at-home $99 genetic analysis kit.[3]

But many other new innovations are also at risk. Federal and state officials are already exploring how to regulate the "Internet of Things," smart cars, commercial drones, 3D printing, and many other new technologies that have barely made it out of the cradle. This text will be peppered with short case studies, or "Innovation Opportunities," that could be endangered by

precautionary principle thinking, especially regulatory efforts rooted in privacy, safety, and security fears.

In extolling these innovation opportunities, I will argue that it is essential to allow them to evolve in a relatively unabated fashion. To be clear, this is not to "protect corporate profits" or to assist any particular technology, industry sector, or set of innovators. Rather, this is about ensuring that individuals as both citizens and consumers continue to enjoy the myriad benefits that accompany an open, innovative information ecosystem. More profoundly, this general freedom to innovate is essential for powering the next great wave of industrial innovation and rejuvenating our dynamic, high-growth economy. Even more profoundly, this is about preserving social and economic freedom more generally while rejecting the central-planning mentality and methods that throughout history have stifled human progress and prosperity.

*Note*: Much of what follows in this book has been adapted from my recent law review articles, filings to federal agencies, editorials, and blog posts. Most of those essays are listed in the appendix, and readers should consult them for a fuller exploration of the issues discussed here.

## NOTES

1. Joshua D. Wright, "DC's Cab Rules Should Put Consumers First," *Washington Post*, September 6, 2013, http://www.washingtonpost.com/opinions/has-the-dc-cab-commission-forgotten-who-it-serves/2013/09/06/cb3d0c18-15a6-11e3-be6e-dc6ae8a5b3a8_story.html.
2. Joe Mullin, "Airbnb Gets Subpoena Demand for Data on All 15,000 NYC-Area Hosts," *Ars Technica*, October 7, 2013, http://arstechnica.com/tech-policy/2013/10/airbnb-gets-subpoena-demand-for-all-data-on-all-15000-nyc-area-hosts.
3. Larry Downes and Paul Nunes, "Regulating 23andMe to Death Won't Stop the New Age of Genetic Testing," *Wired*, January 1, 2014, http://www.wired.com/opinion/2014/01/the-fda-may-win-the-battle-this-holiday-season-but-23andme-will-win-the-war.

# I. INTRODUCTION: WHY PERMISSIONLESS INNOVATION MATTERS

## A: FROM SCARCITY TO ABUNDANCE

Until just recently, humans lived in a state of extreme information poverty. Our ancestors were starved for informational inputs and were largely at the mercy of the handful of information producers and distributors that existed in each era.

The rise of the Internet and the digital economy changed all that.

We are now blessed to live in a world of unprecedented information abundance and diversity. We enjoy a world of hyper-ubiquitous, instantly accessible information and media in which we can access and consume whatever content we want, wherever, whenever, and however we want it.

Better yet, we have access to communications networks and media platforms that give every man, woman, and child the ability to be a publisher and express themselves to the entire planet.

But we ain't seen nothin' yet. We stand on the cusp of the next great industrial revolution and developments that could vastly enhance the welfare of people across the planet.

Yet it will only happen if we preserve the fundamental value that has thus far powered the information age revolution: "permissionless innovation," which refers to the general freedom to experiment and learn through ongoing trial-and-error experimentation.

Just as permissionless innovation powered the Internet and the modern digital revolution, we can have this kind of

dynamism in the rest of the economy as well. There is no reason this ethos should be restricted to today's information sector.

Unfortunately, while many Internet pundits and advocates often extol the permissionless innovation model for the information sector, they ignore its applicability outside that context. That is unfortunate, because we can and should expand the horizons of permissionless innovation in the physical world, too. We need the same revolutionary approach to new technologies and sectors, whether based on bits (the information economy) or atoms (the industrial economy).

The various case studies outlined throughout this text will show how the need to seek permission can harm innovation in the physical world, not just the virtual one. The costs of this forgone innovation are high. Policymakers should not be imposing prophylactic restrictions on the use of new technologies without clear evidence of actual, not merely hypothetical, harm. More often than not, humans adapt to new technologies and find creative ways to assimilate even the most disruptive innovations into their lives.

Certainly, complex challenges exist—safety, security, privacy, etc.—as they always do with new inventions. But there are good reasons to be bullish about the future and to believe that we will adapt to it over time. A world of permissionless innovation will make us healthier, happier, and more prosperous—if we let it.

## B: WHAT IS PERMISSIONLESS INNOVATION?

Even though the many benefits associated with the rise of the commercial Internet and modern digital technologies are only roughly two decades old, we have already come to take these developments for granted. We expect new and more powerful computers, tablets, and smartphones every year. We expect better and faster broadband. We expect more online content, services, and networking platforms. And so on.

Amazingly, each year we get all this and more, most of which we could not have anticipated even a short time ago. Even as we

enjoy this technological cornucopia, we sometimes forget that, not that long ago, information scarcity and limited consumer choice were the norm. We should pause and ask ourselves: How is it that in the span of just the past few decades we have witnessed the greatest explosion in information availability and human connectedness that the world has ever known?

The answer comes down to two words: "permissionless innovation."

Vint Cerf, one of the fathers of the Internet, credits permissionless innovation for the economic benefits that the Net has generated.[1] As an open platform, the Internet allows entrepreneurs to try new business models and offer new services without seeking the approval of regulators beforehand.

But permissionless innovation means much more than that. It refers to the tinkering and continuous exploration that takes place at multiple levels—from professional designers to amateur coders; from big content creators to dorm-room bloggers; from nationwide communications and broadband infrastructure providers to small community network-builders. *Permissionless innovation is about the creativity of the human mind to run wild in its inherent curiosity and inventiveness*. In a word, permissionless innovation is about *freedom*.

Although permissionless innovation has been the secret sauce that fueled the success of the Internet and much of the modern tech economy in recent years, it wasn't always that way. Most online users today are not aware that, until 1989, commercial use of the Internet was prohibited. As a 1982 MIT handbook for the use of ARPAnet, the progenitor of what would become the Internet, warned students:

> It is considered illegal to use the ARPAnet for anything which is not in direct support of government business.… Sending electronic mail over the ARPAnet for commercial profit or political purposes is both anti-social and illegal. By sending such messages, you can offend many people,

> and it is possible to get MIT in serious trouble with the government agencies which manage the ARPAnet.[2]

Thus, before the early 1990s, the Internet remained a noncommercial platform that was mostly a closed club reserved for academics, a handful of technologists and engineers, and assorted government bureaucrats.

Undoubtedly, those commercial restrictions on the Internet were put in place with the best of intentions. Those who imposed restrictions on commercial use of the Internet probably were simply unable to imagine the enormous benefits that would be generated by allowing it to become an open platform for social and commercial innovation.

Regardless, the opportunity costs of those prohibitions were enormous. "Opportunity cost" refers to the forgone benefits associated with any choice or action.[3] When we think about technological innovation, it is vital to keep the concept of opportunity cost in mind. *Every* action—especially political and regulatory action—has consequences. The nineteenth-century French economic philosopher Frédéric Bastiat explained the importance of considering the many unforeseen, second-order effects of economic change and policy.[4] Many pundits and policy analysts pay attention to only the first-order effects—what Bastiat called "the seen"—and ignore the subsequent and often "unseen" effects.

When commercial uses of an important resource or technology are arbitrarily prohibited or curtailed, the opportunity costs of such exclusion may not always be immediately evident. Nonetheless, those "unseen" effects are very real and have profound consequences for individuals, the economy, and society.

In the case of the Internet, a huge opportunity cost was associated with the initial limitations on its use and its commercial development. Only when this mistake was corrected in the early 1990s, through the commercial opening of the Net, did the true opportunity costs of the original restrictions become evident.

As soon as the Net was commercialized, social and economic activity flourished. Innovations like e-mail and web browsers quickly gained widespread adoption. Websites—personal, corporate, and otherwise—exploded. Online commerce took off.

## INNOVATION OPPORTUNITY: THE "INTERNET OF THINGS"

The so-called Internet of Things is emerging and it promises to usher in profound changes that will rival the first wave of Internet innovation.[5] The Internet of Things (IoT) is sometimes viewed as being synonymous with "smart" systems, such as "smart homes," "smart buildings," "smart health," "smart grids," "smart mobility," and so on.[6] As microchips and sensors are increasingly embedded into almost all "smart devices" we own and come into contact with, a truly "seamless web" of connectivity will finally exist.[7]

The promise of the IoT, as described by *New York Times* reporter Steve Lohr, is that "billions of digital devices, from smartphones to sensors in homes, cars and machines of all kinds, will communicate with each other to automate tasks and make life better."[8] According to Cisco, by 2020, 37 billion intelligent things will be connected and communicating.[9] Thus, we are rapidly approaching the point where "everyone and everything will be connected to the network."[10] ABI Research estimates that there are more than 10 billion wirelessly connected devices in the market today and more than 30 billion devices expected by 2020.[11]

The benefits associated with these developments will be enormous. McKinsey Global Institute estimates the potential economic impact of the IoT to be $2.7 trillion to $6.2 trillion per year by 2025[12] and the consultancy IDC estimates that this market will grow at a compound annual growth rate of 7.9 percent between now and 2020, to reach $8.9 trillion.[13] The biggest impacts will be in health care, energy, transportation, and retail services.

Of course, as with every major technological revolution, these advances will be hugely disruptive—for both the economy and social norms. Safety, security, and privacy concerns have already been raised, and the Federal Trade Commission opened a proceeding on the privacy and security implications of the IoT and hosted a workshop on the issue in November 2013. Some critics are already forecasting the equivalent of a privacy apocalypse with the rise of these technologies and have called for preemptive controls.[14]

Sophisticated search engines emerged. And then blogs, social networks, smartphones, tablets, mobile applications, and various other digital devices and services developed so rapidly that it became hard to keep track of them all.[15]

This all was allowed to take place because our default position for the digital economy was "innovation allowed"; in other words, permissionless innovation. No one had to ask anyone for the right to develop these new technologies and platforms.

## C: THE BENEFITS OF THE NEXT GREAT INDUSTRIAL REVOLUTION

But the story of permissionless innovation isn't over, nor is the Internet the only or last great platform for commercial and social innovation.

We stand on the cusp of the next great industrial revolution.[16] Many of the underlying drivers of the digital revolution—massive increases in processing power, exploding storage capacity, steady miniaturization of computing, ubiquitous communications and networking capabilities, the digitization of all data, and more—are beginning to have a profound impact beyond the confines of cyberspace.

What this means is that "meatspace"—the world of atoms and physical things—is primed for the same sort of revolution that the world of bits—the information economy—has undergone over the past two decades. The world of kinetic, ambient, automated computing and networking that has made our digital products and virtual services better, faster, and more ubiquitous is now ready to spread to the physical world. "The past ten years have been about discovering new ways to create, invent, and work together on the Web," notes popular technology writer Chris Anderson in his recent book *Makers*. "The next ten years will be about applying those lessons to the real world."[17]

When all industrial technology has embedded microchips, sensors, and antennas, the promise of an "always-on" and fully customizable world will truly be upon us. It is easy to see why

this Internet of Things or world of "machine-to-machine communications" might spook some people. As noted below, our first reaction to new innovations such as these is often one of fear and trepidation. We assume the worst for a variety of reasons. There are many reasons that pessimism and worst-case scenarios often dominate discussions about new technologies and business practices.

For now it is enough to note that when we imagine an unfolding world of ambient computing, ubiquitous sensors, robots, private drones, and intelligent devices, it is bound to conjure up dystopian sci-fi scenarios of the machines taking over our lives and economy. Equally fear-inducing are the concerns related to safety, security, and especially privacy. Those fears already animate countless books and articles being published today. Section 3 of this text discusses these issues in more detail.

Again, this is where the permission question comes into play for all these new technologies. "The remaining question," notes my Mercatus Center colleague Eli Dourado, "is whether we will welcome them or try to smother them with regulations and arguments over the transitional gains. The best way to ensure a more prosperous future is to eagerly embrace and support the new technologies.…But they may be coming whether we want them or not, so we need to start thinking about how we'll assimilate them into our lives."[18]

We cannot accurately predict how all these tools or platforms will be used in the future, nor can we even forecast the chances that any one of them pans out. Nevertheless, our experience with the net and modern information technology should give us hope that—if innovation and entrepreneurship are allowed to proceed without preemptive hurdles being placed in the way by regulators—these new technologies will have the chance to usher in amazing, life-enriching changes.

## INNOVATION OPPORTUNITY: WEARABLE TECHNOLOGIES

Wearable technologies are networked devices that can collect data, track activities, and customize experiences to users' needs and desires. These devices typically rely on sensor technologies as well as existing wireless networking systems and protocols (Wi-Fi, Bluetooth, near field communication, and GPS) to facilitate those objectives.[19] These technologies are a subset of the Internet of Things, but they deserve special attention because of their potential widespread societal impact.[20]

Many wearable technologies are already on the market today and are used primarily for health and fitness purposes. The so-called quantified self movement refers to individuals who use digital logging tools to continuously track their daily activity and well-being.

In the future, wearable devices and sensor-rich fabric[21] could be used for personal safety and convenience applications, whether at home or out and about in the world. For example, wearable technologies are already being used by many elderly individuals to ensure they can report medical emergencies to caregivers and family members. Medical Body Area Network (MBAN) sensors in professional health care are also set to take off and "will enable patient monitoring information such as temperature to be collected automatically from a wearable thermometer sensor."[22]

In terms of personal convenience, wearables could be used in both homes and workplaces to tailor environmental experiences, such as automatically adjusting lighting, temperature, or entertainment as users move from one space to another. Companies will also use wearables to tailor services to users who visit their establishments. Disney has created a "Magic Band" that can help visitors to their entertainment parks personalize their experiences before they even get to the facilities.[23]

Of course, these technologies raise many safety, security, and especially privacy concerns.[24] The most notable wearable technology on the market today—and the most controversial—is Google Glass.[25] The peer-to-peer surveillance capabilities of Glass and other wearables like the "Narrative" clip-on camera have already spawned a variety of privacy fears.[26] How much data will these devices collect about us? How might they be used? That remains unclear at this point, but equally unclear is how many beneficial uses and applications might flow from such technologies.[27]

In terms of privacy fears and etiquette issues, the power of social norms in this context could become a crucial determinant of the success of wearable

technologies. As noted below, sometimes cultural norms, public pressure, and spontaneous social sanctions are a far more powerful "regulator" of innovations and how people use new tools when compared to laws and regulations.

## NOTES

1. Vinton Cerf, "Keep the Internet Open," *New York Times*, May 24, 2012, http://www.nytimes.com/2012/05/25/opinion/keep-the-internet-open.html.
2. L. Gordon Crovitz, "WeHelpedBuildThat.com," *Wall Street Journal*, July 29, 2012, http://online.wsj.com/article/SB10000872396390443931404577555073157895692.html.
3. Russell Roberts, "Getting the Most out of Life: The Concept of Opportunity Cost," *Library of Economics and Liberty*, February 5, 2007, http://www.econlib.org/library/Columns/y2007/Robertsopportunitycost.html. ("Opportunity cost is what you have to give up to get something.")
4. Frédéric Bastiat, *What Is Seen and What Is Not Seen* (Indianapolis, IN: Liberty Fund, 1848, 1955), http://www.econlib.org/library/Bastiat/basEss1.html.
5. Michael Mandel, "Can the Internet of Everything Bring Back the High-Growth Economy?" Policy Memo (Washington, DC: Progressive Policy Institute, September 2013), 9, http://www.progressivepolicy.org/2013/09/can-the-internet-of-everything-bring-back-the-high-growth-economy. ("Now we are at the next stage of the Internet Revolution, where the physical world gets connected to data, people, and processes. No one can predict the ultimate course of innovative technologies, but it appears that the Internet of Everything has the potential to help revive the high-growth economy.")
6. Ian G. Smith (ed.), *The Internet of Things 2012—New Horizons* (Halifax, UK: Internet of Things European Research Cluster, 2012), 29–31.
7. Dave Evans, "The Internet of Things: How the Next Evolution of the Internet Is Changing Everything," Cisco White Paper (San Jose, CA: Cisco Systems Inc., April 2011), 2, http://www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf.
8. Steve Lohr, "A Messenger for the Internet of Things," *New York Times*, April 25, 2013, http://bits.blogs.nytimes.com/2013/04/25/a-messenger-for-the-internet-of-things.
9. Dave Evans, "Thanks to IoE, the Next Decade Looks Positively 'Nutty,'" *Cisco Blog*, February 12, 2013, http://blogs.cisco.com/ioe/thanks-to-ioe-the-next-decade-looks-positively-nutty.

10. RFID Working Group of the European Technology Platform on Smart Systems Integration, *Internet of Things in 2020: A Roadmap for the Future*, September 5, 2008, 21, http://www.smart-systems-integration.org/public/documents/publications/Internet-of-Things_in_2020_EC-EPoSS_Workshop_Report_2008_v3.pdf.
11. ABI Research, "More Than 30 Billion Devices Will Wirelessly Connect to the Internet of Everything in 2020," May 9, 2013, https://www.abiresearch.com/press/more-than-30-billion-devices-will-wirelessly-conne.
12. James Manyika, Michael Chui, Jacques Bughin, Richard Dobbs, Peter Bisson, and Alex Marrs, "Disruptive Technologies: Advances That Will Transform Life, Business, and the Global Economy," *Insights & Publications*, McKinsey & Company, May 2013, http://www.mckinsey.com/insights/business_technology/disruptive_technologies.
13. Antony Savvas, "Internet of Things Market Will Be Worth Almost $9 Trillion," *CNME*, October 6, 2013, http://www.cnmeonline.com/news/internet-of-things-market-will-be-worth-almost-9-trillion.
14. See generally Bruce Schneier, "Will Giving the Internet Eyes and Ears Mean the End of Privacy?" *Guardian*, May 16, 2013, http://www.guardian.co.uk/technology/2013/may/16/internet-of-things-privacy-google; Mike Wheatley, "Big Brother's Big Data: Why We Must Fear the Internet of Things," *Silicon Angle*, January 10, 2013, http://siliconangle.com/blog/2013/01/10/big-brothers-big-data-why-we-must-fear-the-internet-of-things.
15. Daniel O'Connor of the Computer and Communications Industry Association argues that the Internet "moves markets closer to the 'perfect competition' end of the spectrum" by minimizing barriers to entry, increasing the mobility of labor and capital, expanding information flows, minimizing transaction costs, and maximizing the overall number of buyers and sellers. See Daniel O'Connor, "Rent Seeking and the Internet Economy (Part 1): Why Is the Internet So Frequently the Target of Rent Seekers?" *DisCo blog*, August 15, 2013, http://www.project-disco.org/competition/081513-rent-seeking-and-the-internet-economy-part-1-why-is-the-internet-so-frequently-the-target-of-rent-seekers.
16. Om Malik, "Will Industrial Internet Create More Jobs? GE Thinks Yes," *GigaOm*, October 8, 2013, http://gigaom.com/2013/10/08/will-industrial-internet-create-more-jobs-ge-thinks-yes.
17. Chris Anderson, *Makers: The New Industrial Revolution* (New York: Crown Business, 2012), 17.
18. Eli Dourado, "The Third Industrial Revolution Has Only Just Begun," *EliDourado.com*, October 10, 2012, http://elidourado.com/blog/the-third-industrial-revolution-has-only-just-begun.
19. Rahul Patel, "Where Is Wearable Tech Headed?" *GigaOm*, September 28, 2013, http://gigaom.com/2013/09/28/where-is-wearable-tech-headed.

20. David Evans, "The Future of Wearable Technology: Smaller, Cheaper, Faster, and Truly Personal Computing," *LinkedIn*, October 24, 2013, http://www.linkedin.com/today/post/article/20131024145405-122323-the-future-of-wearable-technology-smaller-cheaper-faster-and-truly-personal-computing.
21. Stacey Higginbotham, "You Call Google Glass Wearable Tech? Heapsylon Makes Sensor-Rich Fabric," *GigaOm*, May 16, 2013, http://gigaom.com/2013/05/16/you-call-google-glass-wearable-tech-heapsylon-makes-sensor-rich-fabric.
22. ABI Research, "Disposable Wireless Sensor Market Shows Signs of Life—Healthcare Shipments to Reach 5 Million in 2018," May 3, 2013, http://www.abiresearch.com/press/disposable-wireless-sensor-market-shows-signs-of-l.
23. Matthew Panzarino, "Disney Gets into Wearable Tech with the MagicBand," *Next Web,* May 29, 2013, http://thenextweb.com/insider/2013/05/29/disney-goes-into-wearable-tech-with-the-magic-band.
24. Hayley Tsukayama, "Wearable Tech Such as Google Glass, Galaxy Gear Raises Alarms for Privacy Advocates," *Washington Post*, September 30, 2013, http://www.washingtonpost.com/business/technology/wearable-technology-raise-privacy-concerns/2013/09/30/0a81a960-2493-11e3-ad0d-b7c8d2a594b9_story.html.
25. Clive Thompson, "Googling Yourself Takes on a Whole New Meaning," *New York Times*, August 30, 2013, http://mobile.nytimes.com/2013/09/01/magazine/googling-yourself-takes-on-a-whole-new-meaning.html?pagewanted=5&_r=0&hpw=&.
26. Liz Gannes, "Narrative—Formerly Known as Memoto—Launches Life-Logging Camera, Raises $3M," *All Things D*, October 3, 2013, http://allthingsd.com/20131003/narrative-formerly-known-as-memoto-launches-life-logging-camera-raises-3m.
27. See generally "Every Step You Take," *Economist*, November 16, 2013, http://www.economist.com/news/leaders/21589862-cameras-become-ubiquitous-and-able-identify-people-more-safeguards-privacy-will-be.

# II. SAVING PROGRESS FROM THE TECHNOCRATS

## A: THOSE WHO FEAR THE FUTURE

Not everyone embraces permissionless innovation. Instead, many critics adopt a mindset that views the future as something that is to be feared and which must be carefully planned. This is known as the "stasis mentality."

In her 1998 book, *The Future and Its Enemies*, Virginia Postrel contrasted the conflicting worldviews of "dynamism" and "stasis" and showed how the tensions between these two visions would affect the course of future human progress.[1] Postrel made the case for embracing dynamism—"a world of constant creation, discovery, and competition"—over the "regulated, engineered world" of the stasis mentality. She argued that we should "see technology as an expression of human creativity and the future as inviting" and reject the idea "that progress requires a central blueprint." Dynamism defines progress as "a decentralized, evolutionary process" in which mistakes aren't viewed as permanent disasters but instead as "the correctable by-products of experimentation."[2] In sum, they are learning experiences.

Postrel notes that our dynamic modern world and the amazing technologies that drive it have united diverse forces in opposition to its continued, unfettered evolution.

> [It] has united two types of stasists who would have once been bitter enemies: reactionaries, whose central value is stability, and technocrats, whose central value is control. Reactionaries seek to reverse change, restoring the literal

> or imagined past and holding it in place.…Technocrats, for their part, promise to manage change, centrally directing "progress" according to a predictable plan.…They do not celebrate the primitive or traditional. Rather, they worry about the government's inability to control dynamism.[3]

Although there are differences at the margin, reactionaries (who tend to be more politically and socially "conservative") and technocrats (who tend to identify as politically "progressive") are united by their desire for greater control over the pace and shape of technological innovation. They both hope enlightened and wise public officials can set us on a supposedly "better path," or return us to an old path from which we have drifted.

Robert D. Atkinson presented another useful way of looking at this divide in his 2004 book, *The Past and Future of America's Economy*:

> This conflict between stability and progress, security and prosperity, dynamism and stasis, has led to the creation of a major political fault line in American politics. On one side are those who welcome the future and look at the New Economy as largely positive. On the other are those who resist change and see only the risks of new technologies and the New Economy. As a result, a political divide is emerging between *preservationists* who want to hold onto the past and *modernizers* who recognize that new times require new means.[4]

Like Postrel's "dynamism versus stasis" paradigm, Atkinson's "preservationists versus modernizers" dichotomy correctly identifies the fundamental conservatism that lies at the heart of the pessimistic attitude and the stasis mentality that dominates among technocrats. The best explanation for this attitude is probably psychological. "We are a conservative species," notes Scott Berkun, author of *The Myths of Innovation*. "Conformity is deep in our biology."[5] This is what psychologists and economists refer to as "loss aversion."

From this stasis-minded perspective, permissionless innovation is undesirable precisely because we can't preserve some of the things that people believe made previous eras or generations great. These could be a specific form of culture, a particular set of institutions or business models, or other norms or values that are rapidly evolving. These critics lament the way modern progress is unfolding because many new technologies are so fundamentally disruptive and are quickly dislodging old standards and institutions.[6] For them, that which is familiar is more comforting than that which is unknown or uncertain.[7] That's the security blanket that the stasis or preservationist mentality provides: the certainty that *un*certainty will be discouraged or even disallowed.

Moreover, because, as Postrel also noted, both reactionaries and technocrats worry about "a future that is dynamic and inherently unstable" and that is full of "complex messiness,"[8] this will lead them to frequently employ fear tactics when debating new technologies and developments.[9] Indeed, both reactionaries and technocrats "claim fear as an ally: fear of change, fear of the unknown, fear of comfortable routines thrown into confusion," Postrel says. "They promise to make the world safe and predictable, if only we will trust them to design the future, if only they can impose their uniform plans."[10] They want to replace this messiness and uncertainty "with the reassurance that some authority will make everything turn out right."[11]

Reactionaries will say we need to control innovation for the sake of order, security, tradition, institutions, and so on. Technocrats will insist that greater control is needed in the name of justice, equality, privacy, and other assorted values. But the ends matter less than the means: Increased control over the course of future developments is the glue that binds both worldviews together in opposition to permissionless innovation.

To simplify matters, we can probably collapse the distinction between these two groups and simply refer to them both as

"technocrats." What they have in common is *how* they seek to gain control over the future course of technological development. Their answer is the "precautionary principle," and it is the antithesis of permissionless innovation.

## B: THE TECHNOCRAT'S TOOL: THE PRECAUTIONARY PRINCIPLE

Ironically, it is *failure* that makes permissionless innovation such a powerful driver of positive change and prosperity.[12] Many social and economic experiments fail in various ways. Likewise, many new technologies fail miserably. *That is a good thing.* We learn how to do things better—both more efficiently and more safely—by making mistakes and dealing with adversity. Challenges and failures also help individuals and organizations learn to cope with change and devise systems and solutions to accommodate technological disruptions.[13]

There's nothing sacrosanct or magical about technology, of course. Technology and technological processes are not an end but the means to achieve many different ends. Just as there is no One Best Way for government to plan a society or economy, there is no One Best Way when humans apply technology to a specific task or set of problems. What makes permissionless innovation so important is that this ongoing process of experimentation and failure helps bring us closer to ideal states and outcomes (more wealth, better health, etc.).

*But we will never discover better ways of doing things unless the process of evolutionary, experimental change is allowed to continue.* We need to keep trying *and even failing* in order to learn how we can move forward. As Samuel Beckett once counseled: "Ever tried. Ever failed. No matter. Try again. Fail again. Fail better."[14] Perhaps the clearest historical example of the logic of "failing better" comes from Thomas Edison, who famously noted of his 10,000 failed lightbulb experiments, "I have not failed 10,000 times. I have not failed once. I have succeeded in proving that those 10,000 ways will not work. When I have

eliminated the ways that will not work, I will find the way that will work."[15]

The value of "failing better" and learning from it was the core lesson stressed by the late political scientist Aaron Wildavsky in his life's work, especially his 1988 book, *Searching for Safety*. Wildavsky warned of the dangers of "trial *without* error" reasoning and contrasted it with the trial-and-error method of evaluating risk and seeking wise solutions to it. Wildavsky argued that real wisdom is born of experience and that we can learn how to be wealthier and healthier as individuals and a society only by first being willing to embrace uncertainty and even occasional failure:

> The direct implication of trial without error is obvious: If you can do nothing without knowing first how it will turn out, you cannot do anything at all. An indirect implication of trial without error is that if trying new things is made more costly, there will be fewer departures from past practice; this very lack of change may itself be dangerous in forgoing chances to reduce existing hazards…. Existing hazards will continue to cause harm if we fail to reduce them by taking advantage of the opportunity to benefit from repeated trials.[16]

When this logic takes the form of public policy prescriptions, it is referred to as the "precautionary principle."[17] The precautionary principle generally holds that, because a new idea or technology could pose some theoretical danger or risk in the future, public policies should control or limit the development of such innovations until their creators can prove that they won't cause any harms.

The problem with letting such precautionary thinking guide policy is that it poses a serious threat to technological progress, economic entrepreneurialism, social adaptation, and long-run prosperity.[18] If public policy is guided at every turn by the precautionary principle, technological innovation is impossible because of fear of the unknown; hypothetical worst-case scenarios trump

all other considerations.[19] Social learning and economic opportunities become far less likely, perhaps even impossible, under such a regime. In practical terms, it means fewer services, lower quality goods, higher prices, diminished economic growth, and a decline in the overall standard of living.[20]

This is why, to the maximum extent possible, the default position toward technological experimentation should be innovation allowed, or permissionless innovation. If we hope to prosper both as individuals and as a society, we must defend the general freedom to experiment and learn through trial and error, and even to fail frequently while doing so.[21]

Stated differently, when it comes to new forms of technological innovation, we need to adopt an "*anti*–precautionary principle" mindset. Legal scholar Paul Ohm, who also recently served as a senior policy advisor at the US Federal Trade Commission, outlined the concept in his 2008 article, "The Myth of the Superuser: Fear, Risk, and Harm Online."[22] "Fear of the powerful computer user, the 'Superuser,' dominates debates about online conflict," Ohm noted, even though this superuser is generally "a mythical figure…whose power has been greatly exaggerated.…Policymakers, fearful of his power, too often overreact by passing overbroad, ambiguous laws intended to ensnare the Superuser but which are instead used against inculpable, ordinary users."[23]

Such "superuser" fears are just the latest variant of hypothetical worst-case scenarios that have long dominated discussions about new innovations. Section 3 discusses some of those past examples. But first, we consider why Chicken Little-ism continues in many discussions about modern technology policy.[24]

### C: WHY DOES DOOMSAYING DOMINATE DISCUSSIONS ABOUT NEW TECHNOLOGIES?

One of the reasons that precautionary thinking often creeps into technology policy discussions is that, as already noted, our collective first reaction to new technologies often is one

of dystopian dread. We assume the worst for a variety of reasons.[25] In the extreme, the initial resistance to new technologies sometimes takes the form of a full-blown technopanic, which refers to "intense public, political, and academic responses to the emergence or use of media or technologies, especially by the young."[26] Some new technologies were initially resisted and even regulated because they disrupted long-standing social norms, traditions, and institutions.

What drives this fear and the resulting panics?

There are many explanations for why we see and hear so much fear and loathing in information technology policy debates today, and even some occasional technopanics.[27] There exist many general psychological explanations for why human beings are predisposed toward pessimism and are risk-averse to new technologies and technological developments.[28] For a variety of reasons, humans are poor judges of risks to themselves or those close to them. Harvard University psychology professor Steven Pinker, author of *The Blank Slate: The Modern Denial of Human Nature*, notes:

> The mind is more comfortable in reckoning probabilities in terms of the relative frequency of remembered or imagined events. That can make recent and memorable events—a plane crash, a shark attack, an anthrax infection—loom larger in one's worry list than more frequent and boring events, such as the car crashes and ladder falls that get printed beneath the fold on page B14. And it can lead risk experts to speak one language and ordinary people to hear another.[29]

Clive Thompson, a contributor to *Wired* and the *New York Times Magazine*, also notes that "dystopian predictions are easy to generate" and "doomsaying is emotionally self-protective: if you complain that today's technology is wrecking the culture, you can tell yourself you're a gimlet-eyed critic who isn't hoodwinked by high-tech trends and silly, popular activities like social networking. You seem like someone who has a richer,

deeper appreciation for the past and who stands above the triviality of today's life."[30]

Beyond these root-cause explanations, there are many other specific factors that contribute to the rise of technopanics and lead us to fear new technological developments. Importantly, however, each of these particular explanations builds on previous insight: Survival instincts combined with poor comparative risk-analysis skills lead many people to engage in, or buy into, technopanics.

- **Generational differences:** Generational differences often motivate pessimistic attitudes about the impact of technology on culture and society. Parents and policymakers who dread the changes to cultural or privacy-related norms ushered in by new technologies often forget they, too, were children once and heard similar complaints from their elders about the gadgets and content of their generation. Yet these cycles of "juvenoia"—or "exaggerated anxiety about the influence of social change on children and youth"—repeat endlessly and drive panics from one generation to the next.[31]
- **Hypernostalgia:** As already noted, many stasis-minded critics just can't seem to let go of the past. They are too invested in it or wedded to something about it. They engage in forms of hypernostalgia and ask us to imagine there existed some earlier time that was more exceptional and valuable than the unfolding present or unpredictable future.[32] Such critics are guilty of both "rosy retrospection bias," or "the tendency to remember past events as being more positive than they actually were,"[33] and a general "pessimistic bias," or "a tendency to overestimate the severity of economic problems and underestimate the (recent) past, present, and future performance of the economy."[34] These critics fear how technological change challenges the old order, traditional values, settled norms, traditional business models, and existing

institutions—even as the standard of living generally improves with each passing generation. We see this at work, for example, in debates about privacy when critics yearn for the supposed solitude of the past, or in copyright debates when critics bemoan the loss of record stores and traditional methods of experiencing music.

- **Bad news sells:** Many media outlets and sensationalist authors sometimes use fear-based tactics to gain influence or sell books. Fearmongering and prophecies of doom are always effective media tactics; alarmism helps media outlets break through all the noise and get heard. This is particularly true as it relates to kids and online safety, where hypothetical threats to children have often dominated media coverage.
- **The role of special interests:** Many groups and institutions exaggerate fears and agitate for action because they benefit from it either directly by getting more resources from government, the public, or other benefactors, or indirectly from the glow of publicity that their alarmism generates. Many companies also overhype various online concerns and then also overplay the benefits of their particular tool as a silver-bullet solution to online pornography, privacy, or cybersecurity concerns. Again, bad news sells—and, in this case, it sells products and services to fearful citizens.
- **Elitist attitudes:** Academic skeptics and cultural critics often possess elitist attitudes about the technologies, platforms, or new types of media content that the masses or youth adopt before they do. These elitist views are often premised on the juvenoia and hypernostalgic thinking described above. Some researchers also have an incentive to perpetuate fear because alarmist research grabs attention and attracts more funding.
- **"Third-person-effect hypothesis":** When some people encounter perspectives or preferences at odds with their

> own, they are more likely to be concerned about the impact of those things on others throughout society and to call on government to "do something" to correct or counter those perspectives or preferences. Psychologists refer to this as the "third-person effect hypothesis," and it explains many technopanics and resulting calls for government intervention, especially as they relate to media policy and free speech issues.[35]

Most technopanics blow over in time, but they can do real harm in the short term. Technopanics can encourage policymakers to adopt far-reaching controls on information flows and innovation opportunities more generally.

## INNOVATION OPPORTUNITY: PRIVATE DRONES

Unmanned aircraft systems (UASs), or drones, are poised to become far more ubiquitous.[36] Private UASs will offer consumers and producers significant benefits, especially in fields such as delivery services and agriculture. Amateur hobbyists and tinkerers may also find many novel uses of private UASs. Private drones could have many important news-gathering uses for both professional media organizations and average citizens.[37]

Unsurprisingly, however, private drones have also raised many safety, security, and privacy concerns.[38] The Federal Aviation Administration (FAA) has already invited comments in a proceeding "addressing the privacy questions raised…[by] unmanned aircraft systems."[39] Legislation limiting private or commercial drone use has already been introduced at the federal level[40] and in many states.[41] Many privacy advocates fear that commercial drones will soon darken our skies and create an omnipresent panopticon.[42]

Some drone regulation is likely inevitable, but preemptive controls could curtail many of the benefits that could flow from relatively unrestrictive experimentation with UASs.[43] Importantly, restrictions on news-gathering uses of private UASs could also raise serious First Amendment concerns.[44] It may be the case that existing laws and policies—property rights, nuisance law, torts, "peeping Tom" laws, etc.—could easily cover most of the scenarios of harm that critics are currently worried about.[45]

Worse yet, continuously elevated states of fear or panic can lead to dangerous tensions throughout society. For example, the past decade witnessed a "stranger danger" panic about hypothetical online bogeymen, leading to overblown suspicions about sexual predators online and even the general presence of males near children.[46] Similarly, excessive panic over cybersecurity matters can lead to paranoia about the potential danger of visiting certain websites or using certain digital tools that are, generally speaking, safe and beneficial to the masses.[47]

The final reason that these fear tactics are dangerous is that they lead to a "risk mismatch." That is, fear-based tactics and inflated threat scenarios can lead to situations where individuals and society ignore quite serious risks because they are overshadowed by unnecessary panics over nonproblems.

## NOTES

1. Virginia Postrel, *The Future and Its Enemies* (New York: Free Press, 1998), xv.
2. Ibid., xiv.
3. Ibid., 7–8.
4. Robert D. Atkinson, *The Past and Future of America's Economy* (Cheltenham, UK: Edward Elgar, 2004), 201 [emphasis added].
5. Scott Berkun, "The Ten Myths of Innovation: The Best Summary," *ScottBerkun.com,* last updated July 7, 2013, http://scottberkun.com/2013/ten-myths-of-innnovation.
6. Dennis Baron, *A Better Pencil: Readers, Writers, and the Digital Revolution* (Oxford, UK: Oxford University Press, 2009), 12 (noting that "the shock of the new often brings out critics eager to warn us away").
7. Aaron Wildavsky, *Searching for Safety* (New Brunswick, CT: Transaction Books, 1988), 54. ("A lot of misplaced nostalgia goes into the (mis)perception that all old, handcrafted items are safer than the new and mass-produced.")
8. Postrel, *The Future and Its Enemies*, xv.
9. See Adam Thierer, "Technopanics, Threat Inflation, and the Danger of an Information Technology Precautionary Principle," *Minnesota Journal of Law, Science & Technology* 14, no. 1 (2013): 312–50.
10. Postrel, *The Future and Its Enemies*, 216.
11. Ibid., 19.
12. This section adapted from Thierer, "Technopanics," 352–79.

13. As Steven Horwitz and Jack Knych observe, "Failure drives change. While success is the engine that accelerates us toward our goals, it is failure that steers us toward the most valuable goals possible. Once failure is recognized as being just as important as success in the market process, it should be clear that the goal of a society should be to create an environment that not only allows people to succeed freely but to fail freely as well." Steven Horwitz and Jack Knych, "The Importance of Failure," *Freeman* 61, no. 9 (November 2011), http://www.fee.org/the_freeman/detail/the-importance-of-failure#axzz2ZnNlpqHQ.
14. Samuel Beckett, *Worstward Ho* (1983).
15. As quoted in Nathan Furr, "How Failure Taught Edison to Repeatedly Innovate," *Forbes*, June 9, 2011, http://www.forbes.com/sites/nathanfurr/2011/06/09/how-failure-taught-edison-to-repeatedly-innovate.
16. Wildavsky, *Searching for Safety*, 38.
17. Thierer, "Technopanics," 309–86.
18. Jonathan H. Adler, "The Problems with Precaution: A Principle without Principle," *American*, May 25, 2011, http://www.american.com/archive/2011/may/the-problems-with-precaution-a-principle-without-principle.
19. Cass R. Sunstein, *Laws of Fear: Beyond the Precautionary Principle* (Cambridge, UK: Cambridge University Press, 2005).
20. Adam Thierer, "Who Really Believes in 'Permissionless Innovation'?" *Technology Liberation Front*, March 4, 2013, http://techliberation.com/2013/03/04/who-really-believes-in-permissionless-innovation.
21. Eli Dourado, "'Permissionless Innovation' Offline as Well as On," *Umlaut*, February 6, 2013, http://theumlaut.com/2013/02/06/permissionless-innovation-offline-as-well-as-on. ("Advocates of the Internet are right to extol the permissionless innovation model—but they are wrong to believe that it need be unique to the Internet. We can legalize innovation in the physical world, too. All it takes is a recognition that real-world innovators should not have to ask permission either.")
22. Paul Ohm, "The Myth of the Superuser: Fear, Risk, and Harm Online," *University of California–Davis Law Review* 41 (2008): 1327–402.
23. Ibid., 1327.
24. See, for example, Schneier, "Giving the Internet Eyes and Ears"; Wheatley, "Big Brother's Big Data"; Sarah A. Downey, "Google Glass Cons: How the Camera-Embedded Eyeglasses Could Shatter Privacy," *Variety*, July 17, 2013, http://variety.com/2013/biz/news/google-glass-cons-how-the-camera-embedded-eyeglasses-could-shatter-privacy-1200563731.
25. This section adapted from Thierer, "Technopanics," 332–47.
26. Ibid., 311.

27. See, for example, Michael Shermer, *The Believing Brain: From Ghosts and Gods to Politics and Conspiracies—How We Construct Beliefs and Reinforce Them as Truths* (New York: Times Books, 2011), 274–75; Bruce Schneier, *Liars & Outliers: Enabling the Trust That Society Needs to Thrive* (Indianapolis, IN: John Wiley & Sons, 2012), 203.
28. See Shermer, *The Believing Brain*, 54, 275. ("Negativity bias: the tendency to pay closer attention and give more weight to negative events, beliefs, and information than to positive.")
29. Steven Pinker, *The Blank Slate: The Modern Denial of Human Nature* (New York: Penguin Books, 2002), 232.
30. Clive Thompson, *Smarter Than You Think: How Technology Is Changing Our Minds for the Better* (New York: Penguin Press, 2013), 283.
31. Adam Thierer, "Why Do We Always Sell the Next Generation Short?" *Forbes*, January 8, 2012, http://www.forbes.com/sites/adamthierer/2012/01/08/why-do-we-always-sell-the-next-generation-short.
32. See generally Thierer, "Technopanics," 335. ("Excessive nostalgia can help explain skepticism about many forms of technological change. It can even result in calls for restrictions on technology.") See also Matt Ridley, *The Rational Optimist: How Prosperity Evolves* (2010), 292. ("There has probably never been a generation since the Paleolithic that did not deplore the fecklessness of the next and worship a golden memory of the past.")
33. Shermer, *The Believing Brain,* 275.
34. Bryan Caplan, *Myth of the Rational Voter: Why Democracies Choose Bad Policies* (Princeton, NJ: Princeton University Press, 2008), 44.
35. Adam Thierer, "Sarkozy, Facebook, Moral Panics & the Third-Person Effect Hypothesis," *Technology Liberation Front*, May 29, 2011, http://techliberation.com/2011/05/29/sarkozy-facebook-moral-panics-the-third-person-effect-hypothesis.
36. Jerry Brito, "Domestic Drones Are Coming Your Way," *Reason.com*, March 11, 2013, http://reason.com/archives/2013/03/11/domestic-drones-are-coming-your-way.
37. Scott Pham, "When Journalism Becomes a Game of Drones," *Mashable*, July 28, 2013, http://mashable.com/2013/07/28/game-of-drones-journalism.
38. Candice Bernd, "The Coming Domestic Drone Wars," *Truthout*, September 19, 2013, http://www.truth-out.org/news/item/18951-the-coming-domestic-drone-wars; Anne Einsenberg, "Preflight Turbulence for Commercial Drones," *New York Times*, September 7, 2013, http://www.nytimes.com/2013/09/08/business/preflight-turbulence-for-commercial-drones.html?pagewanted=all&_r=1&.
39. "Unmanned Aircraft System Test Site Program," 78 Fed. Reg. 12259 (Feb. 22, 2013).

40. Keith Laing, "Sen. Markey Files Bill to Protect Privacy in Commercial Drone Use," *Hill*, November 4, 2013, http://thehill.com/blogs/transportation-report/aviation/189208-sen-markey-files-bill-to-protect-privacy-in-commercial.
41. Lisa Cornwell, "States Consider Regulation of Drones in US Skies," *AP*, August 6, 2013, http://bigstory.ap.org/article/states-consider-regulation-drones-us-skies; Timm Herdt, "California Drone Bill Would Restrict Civilian Use," *Huffington Post*, May 1, 2013, http://www.huffingtonpost.com/2013/05/01/california-drone-bill_n_3191468.html.
42. Andrew Conte, "Drones with Facial Recognition Technology Will End Anonymity, Everywhere," *Business Insider*, May 27, 2013, http://www.businessinsider.com/facial-recognition-technology-and-drones-2013-5.
43. Eli Dourado, "The Next Internet-Like Platform for Innovation? Airspace. (Think Drones)," *Wired*, April 23, 2013, http://www.wired.com/opinion/2013/04/then-internet-now-airspace-dont-stifle-innovation-on-the-next-great-platform.
44. Rob Walker, "The U.S. Government Is Making It Very Difficult for Journalists to Use Drones. That's a Problem," *Yahoo News*, August 28, 2013, http://news.yahoo.com/drone-journalism-faa-restrictions-164543522.html.
45. Kenneth Anderson, "Domestic Drone Regulation for Safety and Privacy," *Volokh Conspiracy*, September 8, 2013, http://www.volokh.com/2013/09/08/domestic-drone-regulation-safety-privacy.
46. See Wendy McElroy, "Destroying Childhood to Save Children," *Freeman*, December 6, 2011, http://www.thefreemanonline.org/headline/destroying-childhood-to-save-children.
47. Adam Thierer, "Achieving Internet Order without Law," *Forbes*, June 24, 2012, http://www.forbes.com/sites/adamthierer/2012/06/24/achieving-internet-order-without-law.

# III. WHAT PROMPTS PRECAUTIONARY THINKING AND POLICY TODAY

In this section, we will move away from the general explanations for what drives fear of new technologies and instead identify some of the specific concerns related to new information technologies and the emerging next great industrial revolution. The most notable concerns relate to privacy, safety, and security.

## A: PLANNING FOR EVERY WORST CASE MEANS THE BEST CASE NEVER COMES ABOUT

Before discussing those concerns, there is one paradox about life in the information age that must be acknowledged: *The Internet giveth and the Internet taketh away*. The great blessing of the Internet and modern digital platforms is that they are highly interconnected, ubiquitous, and generally quite open. Speech and commerce flow freely. On the other hand, you cannot have the most open, accessible, and interactive communications platform that humanity has ever known without also having some serious privacy, security, and safety issues creep up on occasion.

Simply put, openness and interconnectedness offer us enormous benefits, but they also force us to confront gut-wrenching disruptions of both a social and an economic nature. That is the price of admission to this wonderful new world of abundant content and communications opportunities. This tension will only be exacerbated by the rise of the next industrial revolution, the Internet of Things, and an even more interconnected, interactive economy.

Unfortunately, many of the scholars, regulatory advocates, and policymakers who fear the safety, security, and privacy disruptions associated with these changes will often recommend preemptive steps to head off any number of hypothetical worst-case scenarios. Clearly, they have the best of intentions when they recommend such precautionary steps. But we have already identified the most serious flaw in their thinking: *Trying to preemptively plan for every hypothetical worst-case scenario means that many best-case scenarios will never come about*. That is, the benefits that accompany freedom to experiment will necessarily be sacrificed if fear paralyzes our innovative spirit. Progress and prosperity will be stifled as a result.

### INNOVATION OPPORTUNITY: "BIG DATA"

Kenneth Cukier and Viktor Mayer-Schönberger, authors of *Big Data: A Revolution That Will Transform How We Live, Work, and Think*, define big data as "the vast quantity of information now available thanks to the Internet, and which can be manipulated in ways never before possible."[1] These data sets are used to tailor new and better digital services to us and also to target ads to our interests, which helps keep online content and service cheap or free.[2] The Federal Trade Commission has acknowledged these realities, noting: "The growth in mobile and social networking services in particular is striking, and is funded, in part, by the growth of targeted advertising that relies on use of consumer data."[3] This growth is equally true for the "apps economy," which relies heavily on data collection and advertising.[4]

Many of the information services and digital technologies that we already enjoy and take for granted today came about not necessarily because of some initial grand design, but rather through innovative thinking after the fact about how preexisting data sets might be used in interesting new ways.[5] Cukier and Mayer-Schönberger point out that "data's value needs to be considered in terms of all the possible ways it can be employed in the future, not simply how it is used in the present....In the big-data age," they note, "data is like a magical diamond mine that keeps on giving long after its principal value has been tapped."[6] Some examples of such data-driven innovation include language translation tools, mobile traffic services, digital mapping technologies, spam and fraud detection tools,

instant spell-checkers, and more. But big data also powers many life-enriching, even life-saving, services and applications.[9]

Of course, "big data" raises a variety of big privacy and security concerns, leading to calls for new regulations. Various privacy advocates have pushed these efforts, fearing that, without new rules, we will forever lose control of our data or, worse yet, be subjected to new forms of economic or social discrimination.

But if new laws or regulations preemptively curtail data collection based on such fears, innovative new services, devices, and applications might be lost in the future. There are great benefits associated with these data flows and the uses of our personal information, and lawmakers should be careful when seeking to curtail commercial data collection and use or else they could kill the goose that lays the Internet's golden eggs.

The harms that are sometimes alleged about commercial data collection and use are almost never substantiated. No one is being excluded from the information economy or denied new services because of these practices. On the contrary, data collection means all consumers enjoy a fuller range of goods and services, usually at a very low price. Finally, the critics often also ignore the extent to which people adapt to new information technologies and practices over time.

## B: PRIVACY AND DISCRIMINATION CONCERNS

To appreciate how precautionary logic increasingly dominates the public policy dialog about new information technologies, we'll first consider concerns about privacy and "digital discrimination."[7]

Consider a summer 2013 speech by Federal Trade Commission Chairwoman Edith Ramirez on "The Privacy Challenges of Big Data: A View from the Lifeguard's Chair." In it, Ramirez focused her attention on privacy and security fears about the growth of "big data."[8] Ramirez made several provocative assertions in the speech, but the one "commandment" she issued warrants attention. Claiming that "one risk is that the lure of 'big data' leads to the indiscriminate collection of personal information," Ramirez went on to argue:

> The indiscriminate collection of data violates the First Commandment of data hygiene: Thou shall not collect and

> hold onto personal information unnecessary to an identified purpose. Keeping data on the off-chance that it might prove useful is not consistent with privacy best practices. And remember, not all data is created equally. Just as there is low quality iron ore and coal, there is low quality, unreliable data. And old data is of little value.[10]

She continued on, arguing that "information that is not collected in the first place can't be misused" and then outlined a parade of "horribles" that will occur if such data collection is allowed at all.[11] She was particularly concerned that all this data might somehow be used by companies to discriminate against certain classes of customers. Some legal scholars today decry what Ryan Calo of the University of Washington School of Law calls "digital market manipulation," or the belief that "firms will increasingly be able to trigger irrationality or vulnerability in consumers—leading to actual and perceived harms that challenge the limits of consumer protection law, but which regulators can scarcely ignore."[12] Others fear "power asymmetries" between companies and consumers and even suggest that consumers' apparent lack of concern about sharing information means that people may not be acting in their own best self-interest when it comes to online safety and digital privacy choices.[13]

For example, Professor Siva Vaidhyanathan says consumers are being tricked by the "smokescreen" of "free" online services and "freedom of choice."[14] Although he admits that no one is forced to use online services and that consumers can opt out of most of these services or data collection practices, Vaidhyanathan argues that "such choices mean very little" because "the design of the system rigs it in favor of the interests of the company and against the interests of users."[15] He suggests that online operators are sedating consumers using the false hope of consumer choice.[16] "Celebrating freedom and user autonomy is one of the great rhetorical ploys of the global information economy," he says.[17] "We are conditioned to believe that having more choices—empty though they may be—is the very essence

of human freedom. But meaningful freedom implies real control over the conditions of one's life."[18]

Paternalistic claims such as these clash mightily with the foundational principles of a free society—namely, that individuals are autonomous agents who should be left free to make choices for themselves, even when some of those choices strike others as unwise. The larger problem with such claims is, Where does one draw the line in terms of the policy action they seem to counsel? Taken to the extreme, such reasoning would open the door to almost boundless controls on the activities of consumers.

Consumer protection standards have traditionally depended on a clear showing of *actual*, not prospective or hypothetical, harm. It is not enough to claim, "Well, it *could* happen!" In some cases, when the potential harm associated with a particular practice or technology is extreme in character and poses a direct threat to physical well-being, laws have preempted the general presumption that ongoing experimentation and innovation should be allowed by default. But these are extremely rare scenarios, at least in American law, and they mostly involve health and safety measures aimed at preemptively avoiding catastrophic harm to individual or environmental well-being. In the vast majority of other cases, our culture has not accepted that paternalistic idea that the law must "save us from ourselves" (i.e., our own irrationality or mistakes).[19]

But it's not just that this logic rejects personal responsibility, it's that it ignores the costs of preemptive policy action. After all, regulation is not a costless exercise. It imposes profound tradeoffs and opportunity costs that must always be considered.[20]

Unfortunately, many scholars don't bother conducting such a review of the potential costs of their proposals. As a result, preemptive regulation is almost always the preferred remedy to any alleged, hypothetical harm. "By limiting or conditioning the collection of information, regulators can limit market manipulation at the activity level," Calo says.[21] "We could imagine the government fashioning a rule—perhaps inadvisable for

other reasons—that limits the collection of information about consumers in order to reduce asymmetries of information."[22] Ultimately, Calo does not endorse such a rule. Nonetheless, the corresponding cost of such regulatory proposals must be taken into account. If preemptive regulation slowed or ended certain information flows, it could stifle the provision of new and better services that consumers demand.[23]

The views set forth by some of these scholars as well as Chairwoman Ramirez represent a rather succinct articulation of precautionary principle thinking as applied to modern data collection practices. They are essentially claiming that—because there are various privacy risks associated with data collection and aggregation—we must consider preemptive and potentially highly restrictive approaches to the initial collection and aggregation of data.

The problem with that logic should be fairly obvious and it was perfectly identified by Aaron Wildavsky when he noted, "If you can do nothing without knowing first how it will turn out, you cannot do anything at all."[24] Again, the best-case scenarios will never develop if we are gripped with fear by the worst-case scenarios and try to preemptively plan for them with policy interventions.

In his work, Wildavsky correctly noted that "'worst case' assumptions can convert otherwise quite ordinary conditions… into disasters, provided only that the right juxtaposition of unlikely factors occur."[25] In other words, creative minds can string together some random anecdotes or stories and concoct horrific-sounding scenarios about the future that leave us searching for preemptive solutions to problems that haven't even developed yet.

Again, consider Ramirez's speech. When she argues that "information that is not collected in the first place can't be misused," that is undoubtedly true. But it is equally true that information that is not collected at all is information that might have been used to provide us with the next "killer app" or the

great gadget or digital service that we cannot currently contemplate but that some innovative entrepreneur out there might be looking to develop.

Likewise, claiming that "old data is of little value" and issuing the commandment that "thou shalt not collect and hold onto personal information unnecessary to an identified purpose" reveals a rather shocking arrogance about the possibility of serendipitous data discovery. The reality is that the cornucopia of innovative information options and opportunities we have at our disposal today was driven in large part by data collection, including personal data collection. And often those innovations were not part of some initial grand design; instead they came about through the discovery of new and interesting things that could be done with data after the fact.

Examples include many of the information services and digital technologies that we enjoy and take for granted today, such as language translation tools, mobile traffic services, digital mapping technologies, spam and fraud detection tools, and instant spell-checkers. As Viktor Mayer-Schönberger and Kenneth Cukier point out in their recent book, *Big Data: A Revolution That Will Transform How We Live, Work, and Think*, "data's value needs to be considered in terms of all the possible ways it can be employed in the future, not simply how it is used in the present." They note, "In the big-data age, data is like a magical diamond mine that keeps on giving long after its principle value has been tapped."[26]

In any event, if the new policy in the United States is to follow Ramirez's pronouncement that "keeping data on the off-chance that it might prove useful is not consistent with privacy best practices," then much of the information economy as we know it today will need to be shut down. At a minimum, entrepreneurs will have to start hiring a lot more lobbyists who can sit in Washington and petition the FTC or other policymakers for permission to innovate whenever they have an interesting new idea for how to use data to offer a new service other than the

one for which it was initially collected. Again, this is "Mother, may I" regulation, and we had better get used to a lot more of it if we go down the path Ramirez is charting.

It is useful to contrast Ramirez's approach with that of her fellow FTC Commissioner Maureen K. Ohlhausen. In an October 2013 speech titled, "The Internet of Things and the FTC: Does Innovation Require Intervention?" Ohlhausen noted, "The success of the Internet has in large part been driven by the freedom to experiment with different business models, the best of which have survived and thrived, even in the face of initial unfamiliarity and unease about the impact on consumers and competitors."[27]

More importantly, Ohlhausen went on to highlight another crucial point about why the precautionary mindset is dangerous when enshrined into laws or regulations. Put simply, many elites and regulatory advocates ignore *regulator irrationality* or *regulatory ignorance*. That is, they spend so much time focused on the supposed irrationality of consumers and their openness to persuasion or "manipulation" that they ignore the more serious problem of the irrationality or ignorance of those who (incorrectly) believe they are always in the best position to solve every complex problem. Regulators simply do not possess the requisite knowledge to perfectly plan for every conceivable outcome. This is particularly true for information technology markets, which generally evolve much more rapidly than other sectors, and especially more rapidly than the law itself.

That insight leads Ohlhausen to issue a wise word of caution to her fellow regulators:

> It is…vital that government officials, like myself, approach new technologies with a dose of regulatory humility, by working hard to educate ourselves and others about the innovation, understand its effects on consumers and the marketplace, identify benefits and likely harms, and, if harms do arise, consider whether existing laws and regulations are sufficient to address them, before assuming that new rules are required.[28]

This again suggests that Ohlhausen's approach to technological innovation is consistent with the permissionless innovation approach, whereas Ramirez's is based on precautionary principle thinking. Again, this tension dominates almost all policy debates over new technology today, even if it is not always on such vivid display.

The fact is, almost every new media or communications technology raises some sort of privacy-related concern. Although privacy is a highly subjective value, most everyone can find a new technology or service that they find "creepy" because it violates their visceral sense of privacy.[29] But as section 4 will prove, more often than not, we humans prove particularly good at adapting to new technologies and finding ways to sensibly assimilate them into our lives over time. Organizations and individuals find creative ways to collaborate to create empowerment tools and educational initiatives to adjust to technological change.

### C: SAFETY AND SPEECH CONCERNS

Many parents and policymakers worry about how new information technologies and other modern innovations might expose their children to objectionable content or communications. Primary concerns include online pornography, "hate speech," and controversial ideas.[30]

The first great wave of Internet innovation in the early and mid-1990s gave rise to intense online safety concerns. As the Internet expanded quickly in the mid-1990s, a technopanic over online pornography developed just as quickly.[31] Unfortunately, the inflated rhetoric surrounding "the Great Cyberporn Panic of 1995"[32] turned out to be based on a single study with numerous methodological flaws.[33]

Similarly, a decade later, as social networking sites began growing in popularity, in 2005–06 several state attorneys general and lawmakers began claiming that sites like MySpace and Facebook represented a "predators' playground," implying that youth could be groomed for abuse or abduction by visiting

those sites.[34] Regulatory efforts were pursued to remedy this supposed threat, including a proposed federal ban on access to social networking sites in schools and libraries as well as mandatory online age verification, which was endorsed by many state attorneys general.[35] These measures would have affected a wide swath of online sites and services with interactive functionality.[36]

Unsurprisingly, the bill proposing a federal ban on social networks in schools and libraries was titled the Deleting Online Predators Act of 2006.[37] That year, the measure received 410 votes in the US House of Representatives before finally dying in the Senate.[38] The bill was introduced in the following session of Congress, but did not see another floor vote and was never implemented.[39] During this same period, many states floated bills that also sought to restrict underage access to social networking sites. However, none of the underage access restrictions introduced with these bills were ultimately enacted as law.[40]

Despite the heightened sense of fear aroused by policymakers over this issue, there was almost no basis for the predator panic. It was based almost entirely on threat inflation. "As with other moral panics, the one concerning MySpace had more to do with perception than reality," concluded social media researcher Danah Boyd.[41] Furthermore, she states, "As researchers began investigating the risks that teens faced in social network sites, it became clear that the myths and realities of risk were completely disconnected."[42]

Generally speaking, the fear about strangers abducting children online was always greatly overstated, since it is obviously impossible for abductors to directly "snatch" children by means of electronic communication. Abduction after Internet contact requires long-term, and usually long-distance, grooming and meticulous planning about how to commit the crime.[43] This is not to say there were no cases of abduction that involved Internet grooming, but such cases did not represent the epidemic that some suggested.[44]

Lenore Skenazy, author of *Free-Range Kids: Giving Our Children the Freedom We Had without Going Nuts with Worry*, puts things in perspective: "[T]he chances of any one American child being kidnapped and killed by a stranger are almost infinitesimally small: .00007 percent."[45] A May 2010 report by the Department of Justice confirmed that "family abduction [remains] the most prevalent form of child abduction in the United States."[46] These facts are not intended to trivialize the seriousness of abduction by family members or family acquaintances, but they make it clear that the panic over strangers using social networks to groom and abduct children was based on a faulty premise that kidnappings resulting from online grooming by sexual predators are commonplace and demand preemptive Internet controls. Regardless, as with all other technopanics, the predator panic eventually ran its course, although some of the aforementioned fears remain in the public consciousness.

Importantly, many individuals and organizations have worked together to empower and educate the public on how to deal with underage access to objectionable online material.[47] And many industry trade associations and nonprofit advocacy groups have established industry best practices and codes of conduct to ensure users of all ages have a safer and more secure online experience. For example, the Family Online Safety Institute, which coordinates online safety campaigns with various online operator and child safety advocacy groups, sponsors the Broadband Responsibility Awareness Campaign.[48] The effort includes "A Blueprint for Safe and Responsible Online Use" that encourages member organizations to help create a culture of online responsibility by adopting various education and empowerment-based efforts.[49]

Concerns about online hate speech often lead to calls for preemptive speech controls as well.[50] Many academics,[51] pundits,[52] and advocacy groups have pushed governments across the globe to clamp down on various types of offensive online speech. Sometimes, concerns about controversial or potentially

false online information raise similar calls for preemptive action, sometimes in a completely contradictory fashion.

For example, noted Internet critic Evgeny Morozov has argued that online intermediaries should be doing both more and less to police online speech and content. In a January 2012 *Slate* essay, Morozov argued that steps be taken to root out lies, deceptions, and conspiracy theories on the Internet.[53] Morozov was particularly worried about "denialists of global warming or benefits of vaccination," but he also wondered how we might deal with 9/11 conspiracy theorists, the anti-Darwinian intelligent design movement, and those who refuse to accept the link between HIV and AIDS.[54]

He recommended that Google "come up with a database of disputed claims" or "exercise a heavier curatorial control in presenting search results" to weed out such things.[55] He suggested that the other option "is to nudge search engines to take more responsibility for their index and exercise a heavier curatorial control in presenting search results for issues" that someone (he never says who) determines to be conspiratorial or antiscientific in nature.[56]

Yet, less than a year later in a *New York Times* op-ed, Morozov claimed that Silicon Valley is imposing a "deeply conservative" "new prudishness" on modern society.[57] The cause, he says, is "dour, one-dimensional algorithms, the mathematical constructs that automatically determine the limits of what is culturally acceptable."[58] He proposed that some form of external algorithmic auditing be undertaken to counter this supposed problem.

Taken together, Morozov's two essays may initially appear intellectually schizophrenic. Yet what unifies them is his technocratic tendency to think there is some sort of "Goldilocks" formula to getting things just right as they pertain to online free speech. Morozov is vague on the details of his proposed regime, however. "Is it time for some kind of a quality control system [for the Internet]?" he asked in *Slate*. Perhaps that would be the algorithmic auditors he suggests in his *New York Times* essay.

But who, exactly, are those auditors? What is the scope of their powers? Again, like so many other technocratic, precautionary

## INNOVATION OPPORTUNITY: 3-D PRINTING AND ADDITIVE MANUFACTURING

3D printing, or what is more accurately labeled "additive manufacturing," refers to technology that "moves us away from the Henry Ford era mass production line, and will bring us to a new reality of customizable, one-off production."[59] Working from digital blueprints, 3-D printers let users fabricate or replicate almost any product imaginable using various materials.[60]

These devices are just now gaining more widespread adoption and promise to significantly alter the way many goods are manufactured.[61] In mid-2013, Gartner estimated a 49 percent jump in sub-$10,000 3-D printer sales over the previous year and projected sales to double in each of the following two years.[62] "Once we link together innovations like 3D printing, the Internet of Things, and Big Data, the sky's the limit on what we can dream up. We won't just be able to build any object we need—it will instantly become part of our networked world," says Brian Proffitt of *ReadWrite*.[63]

The ramifications of 3-D printing could be enormous. "The Internet changed the balance of power between individuals and institutions," notes digital visionary Esther Dyson, "[and] I think we will see a similar story with 3D printing, as it grows from a novelty into something useful and disruptive—and sufficiently cheap and widespread to be used for (relatively) frivolous endeavors as well. We will print not just children's playthings, but also human prostheses—bones and even lungs and livers—and ultimately much machinery, including new 3D printers."[64] "Very soon," notes Proffitt, "the day will come when a patient in need of a custom medical device, such as a prosthesis or stent, can have such an object manufactured within minutes right at the healthcare facility, instead of waiting for days to get the device delivered from a factory."[65]

But the growth of additive manufacturing has also raised safety fears and concerns about economic dislocations. Others worry about what it might mean for the future of intellectual property when products can be so easily replicated.[66] Meanwhile, proposals to regulate 3-D-printed guns have already been introduced in the state of New York.[67] More efforts to preemptively regulate 3-D printers are likely to surface as additive manufacturing technologies grow more popular.

principle–minded pundits, Morozov refuses to let us in on the details. We are supposed to instead be content to trust him or some group of technocratic philosopher kings to make wise decisions on our behalf and guide online speech and content down some supposedly better path.

### D: SECURITY CONCERNS

Viruses, malware, spam, data breaches, and critical system intrusions are just some of the security-related concerns that often motivate precautionary thinking and policy proposals.[68]

In today's cybersecurity debates, it is not uncommon to hear frequent allusions to the potential for a "digital Pearl Harbor,"[69] a "cyber cold war,"[70] or even a "cyber 9/11."[71] These analogies are made even though these historical incidents resulted in death and destruction of a sort not comparable to attacks on digital networks. Others refer to "cyber bombs" even though no one can be "bombed" with binary code.[72] Michael McConnell, a former director of national intelligence, went so far as to say that the "threat is so intrusive, it's so serious, it could literally suck the life's blood out of this country."[73]

Such statements reflect the frequent use of "threat inflation" rhetoric in debates about online security.[74] Threat inflation has been defined as "the attempt by elites to create concern for a threat that goes beyond the scope and urgency that a disinterested analysis would justify."[75] Meanwhile, similar concerns have already been raised about security vulnerabilities associated with the Internet of Things and networked appliances.[76]

These online security concerns are almost always overblown, however. In his research on the digital security marketplace, my Mercatus Center colleague Eli Dourado has illustrated how we are able to already achieve "Internet Security without Law."[77] Dourado documented the many informal institutions that enforce network security norms on the Internet and shows how cooperation among a remarkably varied set of actors improves online security without extensive regulation or punishing legal

liability. "These informal institutions carry out the functions of a formal legal system—they establish and enforce rules for the prevention, punishment, and redress of cybersecurity-related harms," Dourado says.[78]

For example, a diverse array of computer security incident response teams (CSIRTs) operate around the globe, sharing their research on and coordinating responses to viruses and other online attacks. Individual Internet service providers (ISPs), domain name registrars, and hosting companies work with these CSIRTs and other individuals and organizations to address security vulnerabilities. A growing market for private security consultants and software providers also competes to offer increasingly sophisticated suites of security products for businesses, households, and governments. "Corporations, including software vendors, antimalware makers, ISPs, and major websites such as Facebook and Twitter, are aggressively pursuing cyber criminals," notes Roger Grimes of *Infoworld*.[79] "These companies have entire legal teams dedicated to national and international cyber crime. They are also taking down malicious websites and bot-spitting command-and-control servers, along with helping to identify, prosecute, and sue bad guys," he says.[80]

A great deal of security knowledge is also "crowd-sourced" today via online discussion forums and security blogs that feature contributions from experts and average users alike. University-based computer science and cyberlaw centers and experts have also helped by creating projects like Stop Badware, which originated at Harvard University but then grew into a broader nonprofit organization with diverse financial support.[81]

Dourado notes that these informal, bottom-up efforts to coordinate security responses offer several advantages over top-down government solutions such as administrative regulatory regimes or punishing liability regimes. First, the informal cooperative approach "gives network operators flexibility to determine what constitutes due care in a dynamic environment." "Formal legal standards," by contrast, "may not be able to

adapt as quickly as needed to rapidly changing circumstances," he says.[82] Simply put, markets are more nimble than mandates when it comes to promptly patching security vulnerabilities.

Second, Dourado notes that "formal legal proceedings are adversarial and could reduce ISPs' incentives to share information and cooperate."[83] Heavy-handed regulation or threatening legal liability schemes could have the unintended consequence of discouraging the sort of cooperation that today alleviates security problems swiftly.

Third, legal solutions are less effective because "the direct costs of going to court can be substantial, as can be the time associated with a trial," Dourado argues.[84] By contrast, private actors working cooperatively "do not need to go to court to enforce security norms," meaning that "security concerns are addressed quickly or punishment…is imposed rapidly."[85] For example, if security warnings don't work, ISPs can "punish" negligent or willfully insecure networks by "de-peering," or terminating network interconnection agreements. The very threat of de-peering helps keep network operators on their toes.

Finally, and perhaps most importantly, Dourado notes that international cooperation between state-based legal systems is limited, complicated, and costly. By contrast, under today's informal, voluntary approach to online security, international coordination and cooperation are quite strong. The CSIRTs and other security institutions and researchers mentioned above all interact and coordinate today as if national borders did not exist. Territorial legal system and liability regimes don't have the same advantage; enforcement ends at the border.

Dourado's model has ramifications for other fields of Internet policy. Indeed, as noted above, these collaborative efforts and approaches are already at work in the realms of online safety and digital privacy. Countless organizations and individuals collaborate on empowerment and educational initiatives to improve online safety and privacy. And many industry and nonprofit groups have established industry best practices and codes of

conduct to ensure a safer and more secure online experience for all users. The efforts of the Family Online Safety Institute were discussed above. Another example comes from the Future of Privacy Forum (FPF), a privacy think tank that seeks to advance responsible data practices. The FPF helps create codes of conduct to ensure privacy best practices by online operators and also helps highlight programs run by other organizations.[86] Likewise, the National Cyber Security Alliance helps promote Internet safety and security efforts among a variety of companies and coordinates "National Cyber Security Awareness Month" (every October) and "Data Privacy Day" (held annually on January 28).[87]

What these efforts prove is that not every complex social problem requires a convoluted legal regime or heavy-handed regulatory response. We can achieve *reasonable effective* Internet safety and security without layering on more and more law and regulation. "Dynamic systems are not merely turbulent," Postrel noted. "They respond to the desire for security; they just don't do it by stopping experimentation."[88] She adds, "Left free to innovate and to learn, people find ways to create security for themselves. Those creations, too, are part of dynamic systems. They provide personal and social resilience."[89]

Education is a crucial part of building resiliency in the security context as well. People and organizations can prepare for potential security problems rationally if given even more information and better tools to secure their digital systems and to understand how to cope when problems arise. Again, many corporations and organizations already take steps to guard against malware and other types of cyberattacks by offering customers free (or cheap) security software. For example, major broadband operators such as Comcast and Time Warner Cable offer free antivirus software to customers and various parental control tools to parents.

Thus, although it is certainly true that "more could be done" to secure networks and critical systems, panic is unwarranted

because much is already being done to harden systems and educate the public about risks.[90] Various digital attacks will continue, but consumers, companies, and other organizations are learning to cope and become more resilient in the face of those threats through creative "bottom-up" solutions instead of innovation-limiting "top-down" regulatory approaches.

### E: SUMMARY

Privacy, safety, and security concerns will continue to drive calls for preemptive public policy controls on new forms of technological innovation. But we must not let those fears trump ongoing experimentation and innovation. "There is no way to get increased prosperity without being willing to try new technologies, even if they may sometimes bring short-term questions," notes Michael Mandel, chief economic strategist at the Progressive Policy Institute.[91]

Of course, privacy, safety, and security problems *will* develop. As noted in section 5, companies, advocacy groups, and the government should all work together to educate consumers about proper use and corporate and personal responsibility to head off those problems to the maximum extent possible. When abuse takes place, some rules may become necessary or, more likely, litigation will be used to punish misbehavior, the same way it has in one industry after another and for one technology after another for many years now. There's no reason information technology should be any different in that regard.[92]

But *how* harms are addressed matters deeply. We should exhaust all other potential nonregulatory remedies first—education, empowerment, transparency, etc.—before resorting to preemptive controls on new forms of innovation. In other words, *ex post* (or after the fact) solutions should generally trump *ex ante* (preemptive) controls.

First, however, we will consider the most important reason to be highly skeptical of the preemptive, precautionary principle

mindset: Humans are particularly good at adapting to new technologies and developments.

## NOTES

1. Kenneth Cukier and Viktor Mayer-Schönberger, "The Financial Bonanza of Big Data," *Wall Street Journal*, March 7, 2013, http://online.wsj.com/article/SB10001424127887324178904578343120139164986.html.
2. Joe Weinman, "How Customer Intimacy Is Evolving to Collective Intimacy, Thanks to Big Data," *Forbes*, June 4, 2013, http://www.forbes.com/sites/joeweinman/2013/06/04/how-customer-intimacy-is-evolving-to-collective-intimacy-thanks-to-big-data.
3. Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers* (Washington, DC: Federal Trade Commission, 2010), http://www.ftc.gov/os/2010/12/101201privacyreport.pdf.
4. John Manoogian III, "How Free Apps Can Make More Money Than Paid Apps," *Tech Crunch*, August 26, 2012, http://techcrunch.com/2012/08/26/how-free-apps-can-make-more-money-than-paid-apps.
5. Software & Information Industry Association, "Data-Driven Innovation: A Guide for Policymakers: Understanding and Enabling the Economic and Social Value of Data," May 2013, http://siia.net/index.php?option=com_content&view=article&id=1293:data-driven-innovation&catid=163:public-policy-articles&Itemid=1411.
6. Viktor Mayer-Schönberger and Kenneth Cukier, *Big Data: A Revolution That Will Transform How We Live, Work, and Think* (New York: HMH, 2013): 103–4.
7. This section adapted from Adam Thierer, "Edith Ramirez's 'Big Data' Speech: Privacy Concerns Prompt Precautionary Principle Thinking," *Technology Liberation Front*, August 29, 2013, http://techliberation.com/2013/08/29/edith-ramirezs-big-data-speech-privacy-concerns-prompt-precautionary-principle-thinking; Adam Thierer, "A Framework for Benefit-Cost Analysis in Digital Privacy Debates," *George Mason University Law Review* 20, no. 4 (Summer 2013): 1066–69.
8. Edith Ramirez, "The Privacy Challenges of Big Data: A View from the Lifeguard's Chair," August 19, 2013, http://www.ftc.gov/speeches/ramirez/130819bigdataaspen.pdf.
9. Amy O'Leary, "An App That Saved 10,000 Lives," *New York Times*, October 5, 2013, http://bits.blogs.nytimes.com/2013/10/05/how-to-save-10000-lives-with-an-app-flatter-doctors.
10. Ibid., 4.
11. Ibid., 6.

12. Ryan Calo, "Digital Market Manipulation," *George Washington Law Review* 42 (forthcoming 2014): 5, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2309703. Also see David Talbot, "Data Discrimination Means the Poor May Experience a Different Internet," *MIT Technology Review*, October 9, 2013, http://www.technologyreview.com/news/520131/data-discrimination-means-the-poor-may-experience-a-different-internet.
13. See Anita L. Allen, "Coercing Privacy," *William & Mary Law Review* 40 (1999): 723; Mark MacCarthy, "New Directions in Privacy: Disclosure, Unfairness and Externalities," *I/S: A Journal of Law and Policy for the Information Society* 6 (2011): 443. ("The idea is that individual choice in this area would lead, in a piecemeal fashion, to the erosion of privacy protections that are the foundation of the democratic regime, which is the heart of our political system. Individuals are making an assessment—at least implicitly—of the advantages and disadvantages to them of sharing information. They are determining that information sharing is, on balance, a net gain for them. But the aggregate effect of these decisions is to erode the expectation of privacy and also the role of privacy in fostering self-development, personhood, and other values that underlie the liberal way of life. In this way, individual choices are not sufficient to justify information practices that collectively undermine widely shared public values.")
14. Siva Vaidhyanathan, *The Googlization of Everything (And Why We Should Worry)* (Berkeley, CA: University of California Press, 2011), 83.
15. Ibid., 84.
16. Ibid.
17. Ibid., 89.
18. Ibid.
19. Benjamin R. Sachs, "Comment: Consumerism and Information Privacy: How Upton Sinclair Can Again Save Us from Ourselves," *Virginia Law Review* 95 (2009): 223–26 (arguing that regulation is needed due to the complexity of the information economy and the limits of consumer competence).
20. See Thierer, "A Framework for Benefit-Cost Analysis," 1055–105.
21. Calo, "Digital Market Manipulation," 38.
22. Ibid.
23. Thomas M. Lenard and Paul H. Rubin, "The Big Data Revolution: Privacy Considerations" (Washington, DC: Technology Policy Institute, December 2013), 24, http://www.techpolicyinstitute.org/files/lenard_rubin_thebigdatarevolutionprivacyconsiderations.pdf.
24. Wildavsky, *Searching for Safety*, 38.
25. Ibid., 92.
26. Mayer-Schönberger and Cukier, *Big Data*, 103–4.

27. Maureen K. Ohlhausen, "The Internet of Things and the FTC: Does Innovation Require Intervention?" Remarks before the US Chamber of Commerce, Washington, DC, October 18, 2013, http://www.ftc.gov/speeches/ohlhausen/131008internetthingsremarks.pdf.
28. Ibid.
29. Adam Thierer, "On 'Creepiness' as the Standard of Review in Privacy Debates," *Technology Liberation Front*, December 13, 2011, http://techliberation.com/2011/12/13/on-creepiness-as-the-standard-of-review-in-privacy-debates.
30. This section adapted from Thierer, "Technopanics"; Adam Thierer, "Do We Need a Ministry of Truth for the Internet?" *Forbes*, January 29, 2012, http://www.forbes.com/sites/adamthierer/2012/01/29/do-we-need-a-ministry-of-truth-for-the-internet; Adam Thierer, "Morozov's Algorithmic Auditing Proposal: A Few Questions," *Technology Liberation Front*, November 19, 2012, http://techliberation.com/2012/11/19/morozovs-algorithmic-auditing-proposal-a-few-questions.
31. Robert Corn-Revere, "New Age Comstockery," *CommLaw Conspectus* 4 (1996): 183–84 (analyzing the application of the Communications Decency Act to the Internet).
32. Mike Godwin, *Cyber Rights: Defending Free Speech in the Digital Age*, rev. ed. (Cambridge, MA: MIT Press, 2003), 259.
33. Alice E. Marwick, "To Catch a Predator? The MySpace Moral Panic," *First Monday*, June 2, 2008, http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/2152/1966.
34. Emily Steel and Julia Angwin, "MySpace Receives More Pressure to Limit Children's Access to Site," *Wall Street Journal*, June 23, 2006, B3.
35. Adam Thierer, "Social Networking and Age Verification: Many Hard Questions; No Easy Solutions," *PFF Progress on Point* 14.5 (Washington, DC: Progress & Freedom Foundation, March 21, 2007), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=976936.
36. Adam Thierer, "Would Your Favorite Website Be Banned by DOPA?," *Technology Liberation Front*, March 10, 2007, http://techliberation.com/2007/03/10/would-your-favorite-website-be-banned-by-dopa.
37. Deleting Online Predators Act, H.R. 5319, 109th Cong. (2006). See also Adam Thierer, "The Middleman Isn't the Problem," *Philly.com*, May 31, 2006, http://articles.philly.com/2006-05-31/news/25400396_1_web-sites-social-networking-block-access.
38. 152 Cong. Rec. 16,231 (2006) (referring the bill to the Senate Committee on Commerce, Science, and Transportation); 152 Cong. Rec. 16,040 (2006) (House vote).
39. 153 Cong. Rec. 4,559 (2007) (introducing the bill into the House and referring it to the Committee on Energy and Commerce).

40. The North Carolina bill, as enacted, no longer included the prior access-restriction language. See S. 132, 2007 Gen. Assemb., Reg. Sess. (N.C. 2007) (enacted).
41. See danahmicheleboyd, "Taken out of Context: American Teen Sociality in Networked Publics" (unpublished PhD diss., University of California, Berkeley, 2008), 266, http://www.danah.org/papers/TakenOutOfContext.pdf.
42. Ibid.
43. Samantha Craven, et al., "Sexual Grooming of Children: Review of Literature and Theoretical Considerations," *Journal of Sexual Aggression* 12 (2006): 289 (describing a study in which 45 percent of a sample of convicted child sex offenders had employed sexual grooming behaviors, but also noting that this type of offender may be less likely to be reported, identified, and convicted than more aggressive offenders).
44. Daniel Gardner, *The Science of Fear: How the Culture of Fear Manipulates Your Brain* (2009), 185–86. Gardner states that earlier unfounded statistics estimated 50,000–75,000 children were kidnapped each year, when in fact each year only about 115 "stereotypical kidnappings" (defined as "[a] stranger or slight acquaintance takes or detains a child for ransom or with the intention of keeping him or her, or kills the child") occur in the United States.
45. Lenore Skenazy, *Free-Range Kids: Giving Our Children the Freedom We Had without Going Nuts with Worry* (2009), 16.
46. Office of Juvenile Justice and Delinquency Prevention, US Department of Justice, *The Crime of Family Abduction: A Child's and Parent's Perspective* (Washington, DC, 2010), i, https://www.ncjrs.gov/pdffiles1/ojjdp/229933.pdf.
47. See generally Adam Thierer, *Parental Controls & Online Child Protection: A Survey of Tools and Methods* (Washington, DC: Progress & Freedom Foundation, 2009), http://www.pff.org/parentalcontrols.
48. Family Online Safety Institute, "Initiatives: Broadband Responsibility Awareness Campaign," http://www.fosi.org/initiatives/broadband-responsibility-awareness-campaign.html.
49. Family Online Safety Institute, *Broadband Responsibility: A Blueprint for Safe & Responsible Online Use*, http://www.fosi.org/images/stories/resources/fosi-brac-book-electronic-version.pdf.
50. See Adam Thierer, "The Constructive Way to Combat Online Hate Speech: Thoughts on 'Viral Hate' by Foxman & Wolf," *Technology Liberation Front*, June 24, 2013, http://techliberation.com/2013/06/24/the-constructive-way-to-combat-online-hate-speech-thoughts-on-viral-hate-by-foxman-wolf.
51. Alexander Tsesis, "Dignity and Speech: The Regulation of Hate Speech in a Democracy," *Wake Forest Law Review* 44 (2009).

52. Sean McElwee, "The Case for Censoring Hate Speech," *AlterNet*, July 12, 2013, http://www.alternet.org/civil-liberties/case-censoring-hate-speech.
53. Evgeny Morozov, "Warning: This Site Contains Conspiracy Theories," *Slate*, January 23, 2012, http://www.slate.com/articles/technology/future_tense/2012/01/anti_vaccine_activists_9_11_deniers_and_google_s_social_search_.single.html.
54. Ibid.
55. Ibid.
56. Ibid.
57. Evgeny Morozov, "You Can't Say That on the Internet," *New York Times*, November 16, 2012, http://www.nytimes.com/2012/11/18/opinion/sunday/you-cant-say-that-on-the-internet.html?pagewanted=all&_r=3&.
58. Ibid.
59. Mark Fleming, "What Is 3D Printing? An Overview," *3D Printer*, http://www.3dprinter.net/reference/what-is-3d-printing.
60. See Imran Ali, "The Future of Work: From Bits to Atoms," *GigaOm*, February 10, 2010, http://gigaom.com/2010/02/10/the-future-of-work-from-bits-to-atoms; www.3ders.org, "3D Printing Basics," http://www.3ders.org/3d-printing-basics.html.
61. Signe Brewster, "The Future of Consumer 3D Printing: What's Real, What's Coming, and What's Hype," *GigaOm*, October 2, 2013, http://gigaom.com/2013/10/02/the-future-of-consumer-3d-printing-whats-real-whats-coming-and-whats-hype.
62. John Biggs, "Gartner Estimates Home 3D Printer Shipments Will Grow 49% This Year," *TechCrunch*, October 3, 2013, http://techcrunch.com/2013/10/03/gartner-estimates-home-3d-printer-shipments-will-grow-49-this-year.
63. Brian Proffitt, "How We'll 3D-Print the Internet of Things," *ReadWrite*, October 2, 2013, http://readwrite.com/2013/10/02/3d-printing-internet-of-things#awesm=~oj7KcYZXH93jxD.
64. Esther Dyson, "3D Fantasies," *Project Syndicate*, July 24, 2013, http://www.project-syndicate.org/commentary/how-3d-printing-will-change-the-world-by-esther-dyson.
65. Proffitt, "How We'll 3D-Print."
66. See Deven R. Desai and Gerard N. Magliocca, "3D Printers: The Next Intellectual Property Game Changer," *Philly.com*, October 21, 2013, http://www.philly.com/philly/news/science/3D_printers_The_next_intellectual_property_game_changer.html; Matt Schruers, "3D Printing: Sorry, This Seat Is Reserved," *DisCo (Disruptive Competition)*, February 14, 2013, http://www.project-disco.org/intellectual-property/021413-3d-printing-sorry-this-seat-is-reserved.

67. Dara Kerr, "3D-Printed Guns May Face Regulations, Bans in New York," *CNet.com*, June 13, 2013, http://news.cnet.com/8301-11386_3-57589294-76/3d-printed-guns-may-face-regulations-bans-in-new-york.
68. This section adapted from Adam Thierer, "Achieving Internet Order without Law," *Forbes*, June 24, 2012, http://www.forbes.com/sites/adamthierer/2012/06/24/achieving-internet-order-without-law.
69. See Richard A. Serrano, "Cyber Attacks Seen as a Growing Threat," *Los Angeles Times*, February 11, 2011, A18. ("[T]he potential for the next Pearl Harbor could very well be a cyber attack.")
70. Harry Raduege, "Deterring Attackers in Cyberspace," *Hill*, September 23, 2011, 11, http://thehill.com/opinion/op-ed/183429-deterring-attackers-in-cyberspace.
71. Kurt Nimmo, "Former CIA Official Predicts Cyber 9/11," *InfoWars.com*, August 4, 2011, http://www.infowars.com/former-cia-official-predicts-cyber-911.
72. Rodney Brown, "Cyber Bombs: Data-Security Sector Hopes Adoption Won't Require a 'Pearl Harbor' Moment," *Innovation Report*, October 26, 2011, 10, http://digital.masshightech.com/launch.aspx?referral=other&pnum=&refresh=6t0M1Sr380Rf&EID=1c256165-396b-454f-bc92-a7780169a876&skip=.
73. "Morning Edition: Cybersecurity Bill: Vital Need or Just More Rules?," *NPR*, March 22, 2012, http://www.npr.org/templates/transcript/transcript.php?storyId=149099866.
74. Jerry Brito and Tate Watkins, "Loving the Cyber Bomb? The Dangers of Threat Inflation in Cybersecurity Policy," Mercatus Working Paper 11-24 (Arlington, VA: Mercatus Center at George Mason University, 2011).
75. Jane K. Cramer and A. Trevor Thrall, "Introduction: Understanding Threat Inflation," in *American Foreign Policy and the Politics of Fear: Threat Inflation Since 9/11*, ed. A. Trevor Thrall and Jane K. Cramer (London: Routledge, 2009), 1.
76. Byron Acohido, "Hackers Take Control of Internet Appliances," *USA Today*, October 15, 2013, http://www.usatoday.com/story/cybertruth/2013/10/15/hackers-taking-control-of-internet-appliances/2986395.
77. Eli Dourado, "Internet Security without Law: How Security Providers Create Online Order," Mercatus Working Paper 12-19 (Arlington, VA: Mercatus Center at George Mason University, June 19, 2012), http://mercatus.org/publication/internet-security-without-law-how-service-providers-create-order-online.
78. Ibid.
79. Roger Grimes, "The Cyber Crime Tide Is Turning," *InfoWorld*, August 9, 2011, http://www.pcworld.com/article/237647/the_cyber_crime_tide_is_turning.html.
80. Dourado, "Internet Security."

81. http://stopbadware.org.
82. Dourado, "Internet Security."
83. Ibid.
84. Ibid.
85. Ibid.
86. Future of Privacy Forum, "Best Practices," http://www.futureofprivacy.org/resources/best-practices/.
87. See http://www.staysafeonline.org/ncsam/ and http://www.staysafeonline.org/data-privacy-day.
88. Postrel, *The Future and Its Enemies*, 199.
89. Ibid, 202.
90. Adam Thierer, "Don't Panic over Looming Cybersecurity Threats," *Forbes*, August 7, 2011, http://www.forbes.com/sites/adamthierer/2011/08/07/dont-panic-over-looming-cybersecurity-threats.
91. Michael Mandel, "Can the Internet of Everything Bring Back the High-Growth Economy?," Policy Memo (Washington, DC: Progressive Policy Institute, September 2013), 9, http://www.progressivepolicy.org/2013/09/can-the-internet-of-everything-bring-back-the-high-growth-economy.
92. Antone Gonsalves, "Apple Remote-mobile Device Management Patent Raises Red Flags," *Macworld*, September 2, 2013, http://www.macworld.com.au/news/apple-remote-mobile-device-management-patent-raises-red-flags-106254.

# IV. TAKING ADAPTATION SERIOUSLY

In this section, we consider why our worst fears—both individually and collectively—about new technologies usually do not come to pass. The reason is simple: Humans have the uncanny ability to adapt to changes in their environment, bounce back from adversity, and learn to be resilient over time.

This has important ramifications for the policy debate between the precautionary principle mindset and the notion of permissionless innovation. If adaptation is not just possible but even extremely likely, then there is even less reason to preemptively restrict social and economic experimentation.

## A: FROM PANIC TO EVENTUAL ADAPTATION

Patience and openness to permissionless innovation represent the wise disposition, not only because they provide breathing space for future entrepreneurialism, but also because they provide an opportunity to observe the evolution of societal attitudes toward new technology and see how citizens adapt to them. Citizen attitudes about most emerging technologies likely will follow a familiar cycle we have seen play out in countless other contexts. That cycle typically witnesses initial *resistance*, gradual *adaptation*, and then eventual *assimilation* of a new technology into society.[1]

Again, as noted above, the initial resistance to new technologies sometimes takes the form of a full-blown technopanic. Some new technologies were initially resisted and even regulated because they disrupted long-standing social norms, traditions, and institutions.

Despite these fears, individuals adapted in almost every case and assimilated new technologies into their lives. This is true even for devices and services that initially raised very serious safety, security, or privacy concerns.[2] Technologies that are originally viewed as intrusive or annoying one day often become not just accepted but even essential in fairly short order.

Consider some examples of how society adapted to radical technological change in the past:

- **The telephone:** Many modern media and communications technologies have challenged well-established norms and conventions, but few were as socially disruptive as the telephone. Writing in *Slate*, Keith Collins has noted that "when the telephone was invented, people found the concept entirely bizarre. So much so that the first telephone book, published in 1878, had to provide instructions on how to begin and end calls. People were to say 'Ahoy' to answer the phone and 'That is all' before hanging up," Collins notes.[3] But people quickly adjusted to the new device. "Ultimately, the telephone proved too useful to abandon for the sake of social discomfort," notes Collins. "It was also something people could get used to in their own homes. They didn't have to overcome the awkwardness in public.…That was a barrier another device would have to deal with 100 years later."[4] Of course, when cell phones did come along 100 years later, people got over that "awkwardness," too.
- **Cameras/public photography:** The introduction and evolution of the camera and photography provides another useful example of social adaptation. The camera was viewed as a highly disruptive force when photography became more widespread in the late 1800s. Indeed, the most important essay ever written on privacy law, Samuel D. Warren and Louis D. Brandeis's famous 1890 *Harvard Law Review* essay on "The Right to Privacy," decried the spread of public photography.[5] The authors

lamented that "instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life" and claimed that "numerous mechanical devices threaten to make good the prediction that 'what is whispered in the closet shall be proclaimed from the house-tops.'"[6] But personal norms and cultural attitudes toward cameras and public photography evolved quite rapidly as they became ingrained in human experience. At the same time, social norms and etiquette evolved to address those who would use cameras in inappropriate, privacy-invasive ways.

- **Caller ID:** Although caller identification tools are widely utilized today, they were the subject of a heated privacy debate in the 1990s.[7] The Electronic Privacy Information Center and other privacy advocates wanted the Federal Communications Commission (FCC) to block the revelation of telephone numbers by default, requiring users to opt in to allow their phone numbers to be displayed.[8] Today, caller ID is a routine feature in not just traditional phones but all smartphones.
- **RFID:** When radio-frequency identification (RFID) technologies first came on the scene in the early 2000s, a brief panic followed. Privacy advocates feared that the tracking technology would allow all our movements to be monitored in real time. In the extreme, RFID was likened to the biblical threat of the "mark of the beast."[9] Legislative bills to regulate privacy-related aspects of RFID technology were introduced in several states, although none passed.[10] Fears about RFID were greatly exaggerated and the panic largely passed within a few years.[11] Today, RFID technologies represent the foundation on which many other digital systems and Internet of Things technologies are being developed.[12]
- **Gmail:** When Google launched its Gmail service in 2004, it was greeted with hostility by many privacy advocates

and some policymakers.[13] Rather than charging some users for more storage or special features, Google paid for the service by showing advertisements next to each e-mail, "contextually" targeted to keywords in that e-mail. Some privacy advocates worried that Google was going to "read users' e-mail," however, and pushed for restrictions on such algorithmic contextual targeting.[14] But users enthusiastically embraced Gmail and the service grew rapidly. By the summer of 2012, Google announced that 425 million people were actively using Gmail.[15] Users adapted their privacy expectations to accommodate this new service, which offered them clear benefits (free service, generous storage, and improved search functionality) in exchange for tolerating some targeted advertising.

- **Wireless location-based services:** In Spring 2011, Apple and Google came under fire for retaining location data gleaned by iPhones and Android-based smartphone devices.[16] But these "tracking" concerns were greatly overblown—almost all mobile devices must retain a certain amount of locational information to ensure various services work properly, and these data were not being shared with others.[17] Users who are highly sensitive about locational privacy can always turn off locational tracking or encrypt and constantly delete their data.[18] But most consumers now routinely use wireless location-based services, regardless of privacy concerns.

These case studies prove that, more often than not, society has found ways to adapt to new technological changes by employing a variety of coping mechanisms or new social norms. These examples should give us hope that we will also find ways of adapting to the challenges presented by other new innovations. "Dynamists avoid panic in the face of new ideas," notes Postrel. "They realize that people get used to new developments, that they adjust," she says.[19]

Just as policymakers did not preemptively foreclose innovation with previous information technologies, they should not artificially restrict other forms of innovation today with overly prescriptive privacy, security, or safety regulations. Let innovation continue, and address tangible harms as they develop, if they do at all.

### B: HOW NORMS "REGULATE"

Section 5 considers what role public policy should play in responding to technological disruptions, and other potential solutions. First, it is important to note that new technologies can be regulated by more than law. Social pressure and private norms of acceptable use often act as a "regulator" of the uses (and misuses) of new technologies. This was clearly the case for the uses of the camera, as noted above.

Consider how we are currently witnessing the development of social constraints on mobile phones in various environments. For example, the use of mobile devices in some restaurants and most movie theaters is frowned upon and actively discouraged. Some of these norms or social constraints are imposed by establishments in the form of notices and restrictions on mobile device usage. Some establishments have even created incentives for compliance, by offering discounts for patrons who voluntarily check in their devices.[20] Similar smartphone rules and norms have been established in other contexts; "quiet cars" on trains are one example. Restrictions on the use of camera phones in gym locker rooms is another.

In many cases, these norms or social constraints are purely bottom-up and group-driven. For example, "phone-stacking" refers to a new social convention in which friends having dinner agree to stack their phones in a pile in the middle of the table to minimize distraction. To encourage compliance with the informal rule, the first person who touches his or her phone must pick up the check for the entire table.[21]

Norms are also influenced by the social pressure exerted by advocacy organizations. Media watchdogs and online safety groups have been quite successful in shaping media norms over the past two decades. Groups like Common Sense Media have influenced content decisions through the pressure they have brought to bear on media providers in the marketplace. Common Sense Media not only encouraged and influenced the development of private content rating systems for video games, but the group also developed its own content rating system for games, TV, and movies to provide parents and others with useful information. Similarly, the Parents Television Council (PTC) awards a "seal of approval" to advertisers and programmers that support only programs that the PTC classifies as family-friendly.[22] The organization also encourages parents to send letters and e-mails to advertisers who support programming they find objectionable and encourage those advertisers to end their support of those shows.

In recent years, privacy advocates have also become more visible and gained influence that closely mirrors what occurred with online child safety organizations in the previous two decades. Although both sets of advocates were slow to gain influence at first, their power grew steadily as their respective issues gained more prominence. In addition to their activism and outreach efforts, nonprofit organizations—including the Electronic Privacy Information Center,[23] Privacy Rights Clearinghouse,[24] American Civil Liberties Union,[25] and others—offer instructional websites and tips for how privacy-sensitive consumers can take steps to protect their personal information online. Going forward, we can expect privacy policies—both legal enactments and informal corporate standards—to be significantly influenced by the pressure that these advocates exert on the process.

Finally, the media offers a powerful check on mistakes and misbehavior. Technology developers today face near-constant scrutiny, not just from large media outlets, but also from what

## INNOVATION OPPORTUNITY: AUTONOMOUS VEHICLES AND "SMART CARS"

Our cars are getting smarter and eventually they may all drive themselves so that we don't have to.

The market for "connected cars," or cars that are able to be continuously connected to the Internet, is forecasted to grow from less than one million in 2009 to more than forty-two million by 2017, according to the market research firm iSuppli.[26] And the wireless consultancy *i*GR predicts that between 2012 and 2017, the number of connected cars in the United States will grow by 142 percent. Although the presence of more communications connectivity and media within the cabin of vehicles raises some safety concerns, it also opens up the potential to save lives as those systems making driving safer.

Autonomous or completely "driverless" vehicles could also have many benefits if they are allowed on the roads. "This new technology has the potential to reduce crashes, ease congestion, improve fuel economy, reduce parking needs, bring mobility to those unable to drive, and over time dramatically change the nature of US travel," notes the Eno Center for Transportation.[27] "These impacts will have real and quantifiable benefits," the group notes, because more than thirty thousand people die each year in the United States in automobile collisions, and "driver error is believed to be the main reason behind over 90 percent of all crashes."[28] As Dan Neil of the *Wall Street Journal* sums up: "The promise of autonomy is this: It doesn't have to be perfect, at first, as long as it is better than the faulty, flimsy wetware currently occupying the driver's seat."[29]

More generally, autonomous vehicles could greatly enhance convenience and productivity for average Americans by freeing up time spent behind the wheel. A November 2013 report from Morgan Stanley estimated that autonomous cars could contribute $1.3 trillion in annual savings to the US economy, with global savings estimated at more than $5.6 trillion.[30] A decline in costs for fuel and accidents, as well as $507 billion in annual productivity gains, would drive these savings, notes Morgan Stanley.

Despite these benefits, plenty of critics are already worried about the societal implications of autonomous vehicles.[31] Privacy and safety concerns again dominate. Conflicting state and local laws and liability standards could also greatly limit the growth of these technologies.[32]

Dan Gillmor, author of *We the Media*, refers to as the rise of "we-dia" (user-generated content and citizen journalism) that is an increasingly important part of the modern media landscape.[33] Gillmor, a former *San Jose Mercury News* columnist, speaks of "a modern revolution…because technology has given us a communications toolkit that allows anyone to become a journalist at little cost and, in theory, with global reach. Nothing like this has ever been remotely possible before," he argues.[34] "We are seeing the emergence of new, decentralized approaches to fulfilling the watchdog function and to engaging in political debate and organization," notes Yochai Benkler, author of *The Wealth of Networks*.[35]

This combination of social norms, media attention, and public pressure provides a powerful check on abuses of new technologies.

## NOTES

1. This section adapted from Thierer, "Technopanics," 309–86.
2. Larry Downes, "A Rational Response to the Privacy 'Crisis,'" Policy Analysis 716 (Washington, DC: Cato Institute, January 7, 2013), 10. (Downes has observed, "After the initial panic, we almost always embrace the service that once violated our visceral sense of privacy.")
3. Keith Collins, "OK, Glass, Don't Make Me Look Stupid," *Slate*, May 14, 2013, http://www.slate.com/articles/technology/future_tense/2013/05/google_glass_social_norms_will_it_be_too_awkward_to_use_in_public.html.
4. Ibid.
5. Samuel D. Warren and Louis D. Brandeis, "The Right to Privacy," *Harvard Law Review* 4 (1890): 193.
6. Ibid., 195.
7. S. J. Diamond, "What's behind the Fuss over Caller ID," *Los Angeles Times*, June 15, 1990, http://articles.latimes.com/1990-06-15/business/fi-370_1_caller-id-units; Matthew L. Wald, "Caller ID Reaches Out a Bit Too Far," *New York Times*, February 2, 1995, http://www.nytimes.com/1995/02/02/nyregion/caller-id-reaches-out-a-bit-too-far.html.
8. Electronic Privacy Information Center, "Caller ID," http://epic.org/privacy/caller_id.
9. Mark Baard, "RFID: Sign of the (End) Times?" *Wired*, June 6, 2006, http://www.wired.com/science/discoveries/news/2006/06/70308.

10. Declan McCullagh, "Don't Regulate RFID—Yet," *CNET News*, April 30, 2004, http://news.cnet.com/Don%27t%20regulate%20RFID—yet/2010-1039_3-5327719.html.
11. See generally Jerry Brito, "Relax, Don't Do It: Why RFID Privacy Concerns Are Exaggerated and Legislation Is Premature," *UCLA Journal of Law & Technology* 8 (Fall 2004) (discussing how most fears concerning RFID use are exaggerated).
12. Zhi Zhang, "Networked RFID Systems for the Internet of Things" (doctoral thesis, KTH School of Information and Communication Technology, Stockholm, Sweden, May 2013), http://www.diva-portal.org/smash/get/diva2:613266/FULLTEXT01.
13. See Adam Thierer, "Lessons from the Gmail Privacy Scare of 2004," *Technology Liberation Front*, March 25, 2011, http://techliberation.com/2011/03/25/lessons-from-the-gmail-privacy-scare-of-2004.
14. Letter from Chris Jay Hoofnagle et al. to Bill Lockyer, Attorney General (May 3, 2004), http://epic.org/privacy/gmail/agltr5_3_04.html.
15. Dante D'Orazio, "Gmail Now Has 425 Million Active Users," *Verge*, June 28, 2012, http://www.theverge.com/2012/6/28/3123643/gmail-425-million-total-users.
16. See Kashmir Hill, "Apple and Google to Be the Whipping Boys for Location Privacy," *Forbes*, April 26, 2011, http://www.forbes.com/sites/kashmirhill/2011/04/26/apple-and-google-to-be-the-whipping-boys-for-location-privacy.
17. Brian X. Chen, "Why and How Apple Is Collecting Your iPhone Location Data," *Wired: Gadget Lab*, April 21, 2011, http://www.wired.com/gadgetlab/2011/04/apple-iphone-tracking (explaining how and why Apple uses location data, but pointing out that there was no known reason to keep phones' entire location history in an unencrypted file on the device).
18. See Adam Thierer, "Apple, the iPhone and a Locational Privacy Techno-Panic," *Forbes*, May 1, 2011, http://www.forbes.com/sites/adamthierer/2011/05/01/apple-the-iphone-and-a-locational-privacy-techno-panic.
19. Postrel, *The Future and Its Enemies*, 214.
20. Martha C. White, "Hang up and Eat: Give up Your Cell Phone and Restaurant Discounts Your Meal," *NBC News.com*, August 16, 2012, http://www.nbcnews.com/business/hang-eat-give-your-cell-phone-restaurant-discounts-your-meal-946635.
21. Elie Ayrouth, "Phone Stacking—Is This the Next Phone Etiquette Dining Trend?," *Food Beast*, January 6, 2012, http://foodbeast.com/content/2012/01/06/phone-stacking-is-this-gem-of-social-engineering-the-next-dining-trend.
22. Parents Television Council, http://www.parentstv.org/PTC/awards/main.asp.

23. Electronic Privacy Information Center, "About EPIC," http://epic.org/epic/about.html.
24. Privacy Rights Clearinghouse, "Fact Sheets," https://www.privacyrights.org/privacy-rights-fact-sheets.
25. Nicole A. Ozer, "It's Time to Demand Our dotRights!" ACLU of Northern California, November 18, 2009, https://www.aclunc.org/blog/its-time-demand-our-dotrights.
26. iSuppli Corporation, "Internet: A New Driving Force for Auto Content," *Market Brief* Q4 (2010), http://www.isuppli.com/Abstract/P12409_20110125181525.pdf.
27. Eno Center for Transportation, *Preparing a Nation for Autonomous Vehicles: Opportunities, Barriers and Policy Recommendations* (Washington, DC: October 2013), 17, https://www.enotrans.org/wp-content/uploads/wpsc/downloadables/AV-paper.pdf.
28. Ibid., 3.
29. Dan Neil, "Driverless Cars for the Road Ahead," *Wall Street Journal*, September 27, 2013, http://online.wsj.com/news/articles/SB10001424127887323808204579085271065923340.
30. Morgan Stanley, "Autonomous Cars: Self-Driving the New Auto Industry Paradigm," Morgan Stanley Research, November 6, 2013, http://www.morganstanley.com/public/11152013.html.
31. Patrick Lin, "The Ethics of Saving Lives with Autonomous Cars Are Far Murkier Than You Think," *Wired*, July 30, 2013, http://www.wired.com/opinion/2013/07/the-surprising-ethics-of-robot-cars.
32. See Eno Center, *Preparing a Nation*, 10–14; Joseph B. White, "U.S. Regulators Back Efforts to Develop Cars That Drive Themselves," *Wall Street Journal*, November 19, 2013, http://online.wsj.com/news/articles/SB10001424052702303755504579208700671540562.
33. Dan Gillmor, *We the Media* (Sebastopol, CA: O'Reilly Media, 2004), xii.
34. Ibid., xii.
35. Yochai Benkler, *The Wealth of Networks: How Social Production Transforms Markets and Freedom* (New Haven, CT: Yale University Press, 2006), 11.

# V. PRESERVING PERMISSIONLESS INNOVATION: PRINCIPLES OF PROGRESS

We are now in a position to think more concretely about the policy implications associated with the distinct approaches to thinking about innovation identified above. We can identify four types of responses to new forms of technology and technological risk and plot them along a "risk response continuum." The first two general responses are motivated by the precautionary principle mindset. The latter two are driven by the permissionless innovation vision.[1]

1. **Prohibition:** Prohibition attempts to eliminate potential risk through suppression of technology, product or service bans, information controls, or outright censorship.
2. **Anticipatory regulation:** Anticipatory regulation controls potential risk through preemptive, precautionary safeguards, including administrative regulation, government ownership or licensing controls, or restrictive defaults. Anticipatory regulation can lead to prohibition, although that tends to be rare, at least in the United States.
3. **Resiliency:** Resiliency addresses technological risk through education, awareness building, transparency and labeling, and empowerment efforts.
4. **Adaptation:** Adaptation involves learning to live with risk through trial-and-error experimentation, experience, coping mechanisms, and social norms.

Adaptation strategies often begin with, or evolve out of, resiliency-based efforts.

While these risk-response strategies could also describe the possible range of responses that individuals or families might employ to cope with technological change, generally speaking, we are using this framework to consider the theoretical responses by society at large or by governments.

The adjoining image depicts this range of possible policy responses to new innovations and risks. It illustrates how precautionary or "permissioned" responses (such as prohibition or anticipatory regulation) tend to be more "top-down" in character, focusing on prohibitionary policy solutions or anticipatory regulation. Such solutions tend to be centrally planned and command-and-control in nature.

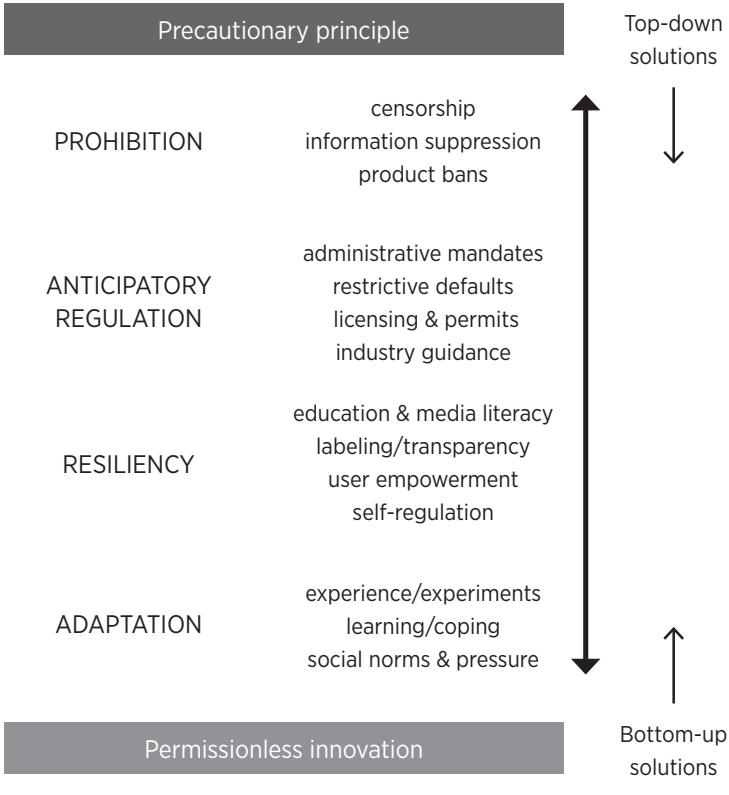
By contrast, permissionless innovation approaches (resiliency and adaptation) are more "bottom-up" in character, evolving more organically in response to new challenges. To summarize the permissionless innovation approach:

1. Society is better off when innovation is not preemptively restricted;
2. Trial-and-error experimentation, the evolution of norms, and the development of educational solutions and coping mechanisms should be the initial responses to new technologies and the risks they pose;
3. Accusations of harm and calls for policy responses should not be premised on hypothetical, worst-case scenarios; and
4. Policy remedies for actual harms should be narrowly tailored so that beneficial uses of technology are not derailed.

We can translate these principles into some general lessons for public policy.

**THE RISK RESPONSE CONTINUUM**

A Range of Responses to Technological Risk




*Source: Adam Thierer, Mercatus Center at George Mason University.*

### A: APPRECIATE THE VIRTUES OF PATIENCE AND FORBEARANCE (OR, "FIRST, DO NO HARM")

At the most abstract level, the most sensible response to a world full of turbulent, dynamic change comes down to patience and tolerance. As Postrel counseled,

> While dynamism requires many private virtues, including the curiosity, risk taking, and playfulness that drive trial-and-error progress, its primary public virtues are those of *forbearance*: of inaction, of not demanding a public ruling on every new development. These traits include tolerance, toughness, patience, and good humor.[2]

This philosophy of forbearance can be applied right down to the individual level, Postrel notes. It comes down to having "the self-restraint not to impose your own idea of the one best way on others [and] not to use political power to short-circuit trial-and-error learning."[3] It is a "tolerance that permits peaceful differences.…It means accepting that we cannot always have things our own way and that we must not limit our neighbors' experiments, aspirations, or ideas just because they might make us feel bad."[4]

More importantly, the philosophy of forbearance should guide public policy. It can take the form of the timeless principle of "first, do no harm." Policymakers should generally exercise restraint and resist the urge to try to plan the future and all the various scenarios—good or bad—that might come about. Again, we earlier saw the philosophy of forbearance at work in the remarks of FTC Commissioner Ohlhausen when she argued for "a dose of regulatory humility" and the need to try harder "to educate ourselves and others about the innovation, understand its effects on consumers and the marketplace, identify benefits and likely harms, and, if harms do arise, consider whether existing laws and regulations are sufficient to address them, before assuming that new rules are required.[5]

## B: LIBERALIZE MARKETS BY APPLYING MOORE'S LAW TO POLICY

One way to translate the philosophy of forbearance into policy is by imposing a variant of "Moore's Law" to technology laws and regulations. Moore's Law is the principle named after Intel cofounder Gordon E. Moore, who first observed that, generally speaking, the processing power of computers doubles roughly every eighteen months while prices remain fairly constant.[6]

Moore's Law has profound ramifications for high-tech policymaking.[7] Technology lawyer and consultant Larry Downes has shown how lawmaking in the information age is inexorably governed by the "law of disruption" or the fact that "technology changes exponentially, but social, economic, and legal systems change incrementally."[8] This law is "a simple but unavoidable principle of modern life," he said, and it will have profound implications for the way businesses, government, and culture evolve going forward. "As the gap between the old world and the new gets wider," he argues, "conflicts between social, economic, political, and legal systems" will intensify and "nothing can stop the chaos that will follow."[9]

To illustrate, consider this cautionary tale told by Jonathan Askin, a technology lawyer and former FCC attorney. In the early 2000s, Askin served as legal counsel to Free World Dialup (FWD), "a startup that had the potential to dramatically disrupt the telecom sector" with its peer-to-peer IP network that could provide free global voice communications.[10] Askin notes that "FWD paved the way for another startup—Skype. But FWD was Skype before Skype was Skype. The difference was that FWD had U.S. attorneys who put the reigns [*sic*] on FWD to seek FCC approvals to launch free of regulatory constraints."[11] Here's what happened to FWD:

> In lightning regulatory speed (18 months), the FCC acknowledged that FWD was not a telecom provider subject to onerous telecom regulations. Sounds like a victory, right? Think again. During the time it took the FCC to

> greenlight FWD, the foreign founders of Skype proceeded apace with no regard for U.S. regulatory approvals. The result is that Skype had a two-year head start and a growing embedded user base, making it difficult for FWD, constrained by its U.S.-trained attorneys, to compete.[12]

FWD would eventually shut down while Skype still thrives.

This shows that no matter how well-intentioned any particular laws or regulations may be, they will be largely ineffective and possibly quite counterproductive when stacked against the realities of the fundamental "law of disruption" because they simply will not be able to keep up with the pace of technological change.[13] "Emerging technologies change at the speed of Moore's Law," Downes notes, "leaving statutes that try to define them by their technical features quickly out of date."[14]

With information markets evolving at the speed of Moore's Law, we should demand that public policy do so as well. We can accomplish that by applying this law to all current and future technology policy laws and regulations through two simple principles:

- **Principle #1:** Every new technology proposal should include a provision sunsetting the law or regulation eighteen months to two years after enactment. Policymakers can always reenact the rule if they believe it is still sensible.
- **Principle #2:** Reopen all existing technology laws and regulations and reassess their worth. If no compelling reason for their continued existence can be identified and substantiated, those laws or rules should be repealed within eighteen months to two years. If a rationale for continuing existing laws and regulations can be identified, the rule can be reimplemented and Principle #1 applied to it.

If critics protest that some laws and regulations are "essential" and they can make the case for new or continued action,

Congress can always legislate to continue those efforts. But when they do, they should always include a two-year sunset provision to ensure that those rules and regulations are given a frequent fresh look.

Better yet, we should just be doing a lot less legislating and regulating in this arena. The only way to ensure that more technologies and entrepreneurs don't end up like FWD is to make sure they don't have to deal with mountains of regulatory red tape from the beginning.

### C: EMBRACE "EDUCATE AND EMPOWER"–BASED SOLUTIONS

"Legislate and regulate" responses are not productive approaches to safety, security, or privacy concerns because preemptive and prophylactic regulation of technology can be costly, complicated, and overly constraining. The better approach might be labeled "educate and empower," which refers to strategies that can help build individual resiliency and ensure proper assimilation of new technologies into society. This approach is built on media literacy and "digital citizenship" and focuses on encouraging better social norms and coping strategies.[15]

For example, regarding online safety and proper online behavior, we need to assimilate children gradually into online environments and use resiliency strategies to make sure they understand how to cope with the challenges they will face in the digital age. Teaching our kids smarter online hygiene and "Netiquette" is vital. "Think before you click" should be lesson number one. They should also be encouraged to delete unnecessary online information occasionally.[16]

In recent years, many child safety scholars and child development experts have worked to expand traditional online education and media literacy strategies, to place the notion of digital citizenship at the core of their lessons.[17] Online safety expert Anne Collier defines digital citizenship as "critical thinking and ethical choices about the content and impact on oneself, others,

and one's community of what one sees, says, and produces with media, devices, and technologies."[18]

This approach should be at the center of child safety debates going forward to encourage ethical online behavior and promote online civility and respect. Only by teaching our children to be good cybercitizens can we ensure they are prepared for life in an age of information abundance.

Many of these same principles and strategies can help us address privacy concerns for both kids and adults. "Again, the solution is critical thinking and digital citizenship," argues online safety expert Larry Magid.[19] He continues, "We need educational campaigns that teach kids how to use whatever controls are built-in to the browsers, how to distinguish between advertising and editorial content and how to evaluate whatever information they come across to be able to make informed choices."[20]

Companies also have an important role to play in creating "well-lit neighborhoods" online where kids will be safe and others can feel their privacy is relatively secure. Many companies and trade associations are also taking steps to raise awareness among their users about how they can better protect their privacy and security.[21] Online operators should also be careful about what (or how much) information they collect—especially if they primarily serve young audiences. Most widely trafficked social networking sites and search engines already offer a variety of privacy controls and allow users to delete their accounts.

Many other excellent online safety- and privacy-enhancing tools already exist for people seeking to safeguard their child's online experiences or their own online privacy. A host of tools are available to block or limit various types of data collection, and every major web browser has cookie-control tools to help users manage data collection. Many nonprofits—including many privacy advocates—offer instructional websites and

videos explaining how privacy-sensitive consumers can take steps to protect their personal information online.

Taken together, this amounts to a "layered approach" to online safety and privacy protection. Only by using many tools, methods, strategies, social norms, and forms of market pressure can we ensure that youngsters and even adults are safe online while they learn to cope with new technology and adapt to the changing world around them.

Governments can play a role in this by facilitating learning and resiliency through educational and empowerment-based solutions, instead of heavy-handed, silver-bullet regulatory solutions. Governments are uniquely positioned to get the word out about new technologies—both the benefits and dangers—and can develop messaging—especially to youngsters still in school—about appropriately using new technologies. For example, the Federal Trade Commission hosts a collaborative online education effort with more than a dozen other federal agencies called "OnGuard Online," which presents a savvy approach to raising awareness about various online threats.[22]

Beyond classroom media literacy and digital citizenship efforts, government can undertake broad-based public awareness campaigns. Officials at the federal, state, and local levels should work together to devise media literacy campaigns focused on online safety, understanding the existing rating systems, how to use parental controls, and so on. These campaigns should include broadcast (radio and TV) ads, Internet websites and advertising, and promotional posters and brochures that could be distributed at schools and government institutions. Government has undertaken (or lent its support to) such public awareness campaigns to address other concerns in the past and had a great deal of success, including forest fire prevention (i.e., "Smokey the Bear");[23] anti-littering ("Give a Hoot, Don't Pollute");[24] crime prevention ("McGruff the Crime Dog");[25] and seat-belt safety.[26]

### D: ENCOURAGE PRIVACY, SAFETY AND SECURITY "BY DESIGN" EFFORTS

One of the hottest concepts in the field of information policy today is "privacy by design."[27] This term refers to efforts by organizations to "embed privacy into the architecture of technologies and practices."[28] There already have been amazing strides made in this regard, and progress—though slow—will continue. "The signs are already beginning to appear," says Ann Cavoukian, who is widely credited with coining the phrase: "Market leaders are embracing *Privacy by Design*, and are, in turn, reaping the benefits."[29] Examples of privacy by design would include efforts by designers and vendors to ensure that consumers know what data are being collected about them and why, making reasonable efforts to protect user confidentiality and secure consumer data, and asking for explicit permission from consumers before sharing information with third parties.[30]

The growth of privacy-by-design efforts reflects a renewed focus on evolving industry self-regulation and codes of conduct. Policymakers and the general public are increasingly demanding that privacy professionals be included in information-gathering institutions and take steps to better safeguard private information flows.[31] The rapid expansion of the ranks of the International Association for Privacy Professionals (IAPP) reflects that fact.[32] The IAPP was formed in 2000 and has rapidly grown from just a few hundred members to almost 14,000 members in 83 countries by 2013.[33] As a result, a growing class of privacy professionals exists throughout the corporate world, as Professors Kenneth Bamberger and Deirdre Mulligan summarize:

> The individuals managing corporate privacy have an applicant pool of trained professionals to draw from. There is ongoing training, certification, and networking. A community of corporate privacy managers has emerged. Ready evidence suggests that substantial effort is made to manage privacy.[34]

But these efforts aren't limited to privacy. Similar efforts have been under way for many years on the online safety front. Various online safety advocates and child safety experts have pushed companies to adopt various online safety best practices to ensure that digital sites and services offer users safer online experiences.[35] Similar "security by design" efforts have been going on for years as well.[36] Corporations and other organizations have a vested interest in keeping their systems and devices secure from viruses, malwares, breaches, spam, and so on.

We should continue to consider how we might achieve privacy by design before new services are rolled out, but the reality is that "privacy on the fly" and "privacy by ongoing norm-shaping" may become even more essential. This is where the role of privacy, safety, and security professionals will be absolutely essential.[37] As Bamberger and Mulligan have noted, increasingly, it is what happens "on the ground"—the day-to-day management of privacy and security decisions through the interaction of privacy and security professionals, engineers, outside experts, and regular users—that is really important. They stress how "governing privacy through flexible principles" is the new norm.[38] They note that "privacy work takes many forms in the firm" today, with privacy professionals responding on the fly to breaking developments, many of which could not have been foreseen.[39] To continuously improve on this model, they argue that the "daily work [of privacy professionals] requires trusted insider status" and "full and early access and ongoing dialogue with business units."[40] Success, they note, "is best accomplished by a diverse set of distributed employees with privacy training who are nonetheless viewed as part of the business team."[41]

That is exactly right. Moreover, going forward, privacy and safety professionals within firms and other organizations will need to be on the front lines of this rapidly evolving technological landscape to solve the hard problems presented by new technologies, such as the Internet of Things, wearable technologies, 3-D printing, and private drones. These professionals will

need to respond to user concerns and continually refine corporate practices to balance the ongoing services that the public demands against the potentially negative impact associated with these technologies. They will need to be creative about data use and deletion policies and simultaneously work to educate the public about appropriate use of these new tools.

### E: RELY ON "SIMPLE RULES FOR A COMPLEX WORLD" WHEN REGULATION IS NEEDED

But don't we need *some* regulation? Yes, of course we do. Regulation is sometimes needed to prevent the harms that businesses or other organizations might impose on customers or third parties. But *how* we prevent or remedy those harms matters profoundly.

We should first look to the sort of less-restrictive remedies to complex social problems described above before we resort to heavy-handed, legalistic solutions. Let us briefly recall the problem with traditional regulatory systems. These tend to be overly rigid, bureaucratic, inflexible, and slow to adapt to new realities. They focus on preemptive remedies that aim to predict the future and future hypothetical problems that may not ever come about. Worse yet, administrative regulation generally preempts or prohibits the beneficial experiments that yield new and better ways of doing things.[42] Regardless of whether the technical specifications for permitted products and services are published in advance or firms must seek special permission before they offer a new product or service, both varieties of preemptive regulation have the same effect: they raise the cost of starting or running a business or nonbusiness venture, and therefore they discourage activities that benefit society.

This is why flexible, "bottom-up" approaches to solving complex problems, such as those outlined in the preceding sections, are almost always superior. For example, we have already identified how social norms and pressure from the public, media, or activist groups can "regulate" behavior and curb potential

abuses. And we have seen how education, awareness-building, transparency, and empowerment-based efforts can often help alleviate the problems associated with new forms of technological change.

But there are other useful approaches that can be tapped to address or alleviate concerns or harms associated with new innovations. To the extent that other *public* policies are needed to guide technological developments, simple legal principles are greatly preferable to technology-specific, micromanaged regulatory regimes. Ex ante (preemptive and precautionary) regulation is often highly inefficient, even dangerous. Prospective regulation based on hypothesizing about future harms that may never materialize is likely to come at the expense of innovation and growth opportunities. To the extent that any corrective action is needed to address harms, ex post measures, especially via the common law, are typically superior.

In his 1983 book, *Technologies of Freedom: On Free Speech in an Electronic Age*, political scientist Ithiel de Sola Pool offered a passionate defense of technological freedom and freedom of speech in the electronic age. He set forth several "Guidelines for Freedom" to ensure that new information technologies could realize their full potential. Regarding regulation of information markets, Pool stressed that "enforcement must be after the fact, not by prior restraint" and that "regulation is a last recourse. In a free society, the burden of proof is for the least possible regulation of communication."[43] That same principle can and should be applied to all technologies more generally.

What we should strive for—to borrow the title of Richard Epstein's 1995 book—are "simple rules for a complex world."[44] Many laws already exist that can be applied to new challenges before we look to impose new laws or more heavy-handed regulation. Those simple rules include the following:

- **Torts, common law, and class-action activity:** The common law of tort is centuries old and well tested. Under tort law, instead of asking for permission to introduce a

potentially dangerous product, a firm must pay for the damages its dangerous product creates if it is found liable in court. Thus, because the tort system operates retrospectively, it is restitution-based, not permission-based. This also creates incentives for firms to make their products safer over time so they can avoid lawsuits.

It is also important to remember how the United States "has a vibrant privacy litigation industry, led by privacy class actions."[45] Class-action lawsuit activity is remarkably intense following not just major privacy violations but also data breaches,[46] and there is evidence that "[h]ow federal courts define the damages people suffer from data breaches is broadening dramatically, leaving unprepared companies at greater risk of big payouts in class-action lawsuits."[47] This disciplines firms that violate privacy and data-security norms while sending a signal to other online operators about their data policies and procedures.[48]

Finally, specific privacy-related torts—including the tort of intrusion upon seclusion—could also evolve in response to technological change and provide more avenues of recourse to plaintiffs seeking to protect their privacy and data security.

- **Property law and other targeted remedies:** Federal and state laws already exist that could address perceived harms associated with many of the new technologies identified herein. For example, property law already governs trespass, and new court rulings may well expand the body of such law to encompass trespass by focusing on actual cases and controversies, not merely hypotheticals. Likewise, many states have "peeping Tom" laws on the books that prohibit spying into homes and other spaces.[49] Anti-harassment laws in every state address such activity. These laws could be adapted to cover developing privacy, safety, and security concerns before new regulations are enacted.

- **Contract law:** The enforcement of contractual promises is one of the most powerful ways to curb potential abuses of new technologies. When companies make promises to the public about new services or devices, the companies can and should be held to them. Again, class-action lawsuits could come into play when firms do not live up to the promises they make to consumers.
- **FTC enforcement of "unfair and deceptive practices":** There are ways outside the courts to ensure that contractual promises are kept. The US Federal Trade Commission possesses broad consumer protection powers under Section 5 of the Federal Trade Commission Act.[50] Section 5 prohibits "unfair or deceptive acts or practices in or affecting commerce."[51] The FTC formalized its process for dealing with unfairness claims in its 1980 *Policy Statement on Unfairness* and noted, "To justify a finding of unfairness the injury must satisfy three tests. It must be substantial; it must not be outweighed by any countervailing benefits to consumers or competition that the practice produces; and it must be an injury that consumers themselves could not reasonably have avoided."[52] (Importantly, however, the *Policy Statement* clarified the meaning of "substantial," stating that "the Commission is not concerned with trivial or merely speculative harms.…Emotional impact and other more subjective types of harm…will not ordinarily make a practice unfair."[53]) In recent years, the FTC has brought and settled many cases involving its Section 5 authority to address identity theft and data-security matters and, generally speaking, has been able to identify clear harms in each case.[54]

  Moreover, targeted legislation already addresses the special concerns raised by the collection or use of certain types of health information,[55] financial information,[56] or information about children.[57] Of course, it is true that the

potential privacy or data-security harms in those contexts are somewhat more concrete in nature. Privacy violations of health and financial information, for example, can pose a more direct and quantifiable threat to personal well-being or property. Finally, state governments and state attorneys general also continue to advance their own privacy and data-security policies, and those enforcement efforts are often more stringent than federal law.[58]

- **Transparency:** If regulation is still deemed necessary, transparency and disclosure policies should generally trump the use of more restrictive rules. The push for better transparency has already led to progress in other contexts. Voluntary media content ratings and labels for movies, music, video games, and smartphone apps have given parents more information to make determinations about the appropriateness of content they or their children may want to consume.[59] And the push for better privacy information has led to more website privacy policies and disclosure statements. Consumers are better served when they are informed about online privacy and data-collection policies of the sites they visit and the devices they use.[60]

### F: QUANTIFY OPPORTUNITY COSTS BY REQUIRING STRICT BENEFIT-COST ANALYSIS

Finally, even when rules are deemed necessary, it does not mean they should be imposed without reference to the potential costs to consumers, industry, or progress and liberty more generally. We need to make sure that new rules make sense and that the "bang for the buck" is real, regardless of the concern being addressed by new laws or regulations.[61]

As discussed in section 2, many cognitive biases predispose us toward pessimism and the precautionary principle mentality. We obviously don't want anything to go wrong and, therefore, many people often call for "steps to be taken" to head off

troubles they believe lie ahead. But, as noted, all policy choices entail trade-offs and have serious opportunity costs.

Legal scholar and risk-analysis expert Cass Sunstein has written of "tradeoff neglect," or the general fact that "people fail to see the frequent need to weigh competing variables against one another."[62] Sunstein correctly observes that "people neglect the systemic effect of one-shot interventions" and instead "tend to assume that a change in a social situation would alter the part at issue but would not affect other parts."[63] In other words, all actions have consequences—especially policy interventions—but we often fail to consider the full extent of the opportunity costs at work.

Bastiat's "seen and unseen" insights are worth recalling in this regard. People often discount unseen gains or opportunities and focus only on the immediately visible benefits or costs. When we choose one course of action it necessarily means we have forgone others. As noted earlier, politicians are often engaged in an elusive search for some magical "Goldilocks" formula to get things "just right" and preempt potential risks. But when we allow our leaders to ignore the opportunity costs of their actions, progress is stunted or at least artificially skewed.

The reality of opportunity costs and trade-off neglect are particularly important to keep in mind when thinking about digital technology and information production and dissemination. These are probably the last technologies and sectors we would want regulators monkeying with, because planners lack the requisite knowledge of how to best guide the evolution of complex, dynamic, fast-moving information technologies. Moreover, the opportunity costs associated with error could be profound and could derail the innovative, informative benefits that have thus far flowed from a largely unregulated digital sphere.

This is why it is essential that all proposals to regulate new technologies be subjected to strict benefit-cost analysis (BCA). BCA represents an effort to formally identify the trade-offs or

opportunity costs associated with regulatory proposals and, to the maximum extent feasible, quantify those benefits and costs.[64]

At the federal level in the United States, regulatory policymaking and the BCA process are directed by various presidential executive orders and guidance issued by the White House Office of Information and Regulatory Affairs (OIRA).[65] As part of any BCA review, OIRA demands "[a] statement of the need for the regulatory action" that includes "a clear explanation of the need for the regulatory action, including a description of the problem that the agency seeks to address."[66] As part of this step, OIRA specifies, "Agencies should explain whether the action is intended to address a market failure or to promote some other goal."[67] Second, "[a] clear identification of a range of regulatory approaches" is required, "including the option of not regulating."[68] Agencies must also consider alternatives to federal regulation, such as "state or local regulation, voluntary action on the part of the private sector, antitrust enforcement, consumer-initiated litigation in the product liability system, and administrative compensation systems."[69] Agencies are supposed to assess the benefits and costs of all these alternatives.[70] If federal regulation is still deemed necessary, flexible approaches are strongly encouraged by OIRA.[71] Finally, "[a]n estimate of the benefits and costs—both quantitative and qualitative" is required.[72] The quantification of benefits and costs is strongly encouraged, but when that is impossible, agencies are required to describe them qualitatively and make a clear case for action.[73]

Unfortunately, federal agency officials often ignore those requirements, or at least do not take them seriously enough. Worse yet for technology policy matters is the fact that many agencies, including the FTC and the FCC, are neither required to conduct BCA nor have their rulemaking activities approved by OIRA. This is like giving regulators a free pass to meddle with new innovation without any serious oversight.

*All* new proposed regulatory enactments should be subjected to strict BCA and, if they are formally enacted, they should

also be retroactively reviewed to gauge their cost-effectiveness. Better yet, the sunsetting guidelines recommended above should be applied to make sure outdated regulations are periodically removed from the books so that innovation is not discouraged. Of course, as already noted above, every effort should be made to exhaust all other options before even entertaining a discussion about the need for new regulations and restrictions on technological innovation. Again, the default should be *innovation allowed*.

## G: SUMMARY

In sum, we need *flexible*, *adaptive* policies and approaches going forward. We need diverse solutions for a diverse citizenry. We must avoid approaches that are top-down, one-size-fits-all, overly rigid, and bureaucratic. Instead, we need approaches that are bottom-up, flexible, and evolutionary in nature.

The challenges ahead will be formidable, but the payoff to society for getting this balance right will be enormous.

## NOTES

1. This section adapted from Thierer, "Technopanics," 352–68.
2. Postrel, *The Future and Its Enemies*, 212 (emphasis in original).
3. Ibid.
4. Ibid., 213.
5. Ohlhausen, "The Internet of Things."
6. "Definition of Moore's Law," *PC Magazine Encyclopedia*, http://www.pcmag.com/encyclopedia_term/0,,t=&i=47229,00.asp.
7. This section adapted from Adam Thierer, "Sunsetting Technology Regulation: Applying Moore's Law to Washington," *Forbes*, March 25, 2012, http://www.forbes.com/sites/adamthierer/2012/03/25/sunsetting-technology-regulation-applying-moores-law-to-washington.
8. Larry Downes, *The Laws of Disruption: Harnessing the New Forces That Govern Life and Business in the Digital Age* (New York: Basic Books, 2009), 2.
9. Ibid., 2–3. In a similar sense, Andy Grove, former CEO of Intel, once reportedly said that "high tech runs three-times faster than normal businesses. And the government runs three-times slower than normal businesses. So we have a nine-times gap." Lillian

Cunningham, "Google's Eric Schmidt Expounds on His Senate Testimony," *Washington Post*, October 1, 2011, http://www.washingtonpost.com/national/on-leadership/googles-eric-schmidt-expounds-on-his-senate-testimony/2011/09/30/gIQAPyVgCL_story.html.

10. Jonathan Askin, "A Remedy to Clueless Tech Lawyers," *Venture Beat*, November 13, 2013, http://venturebeat.com/2013/11/13/a-remedy-to-clueless-tech-lawyers.
11. Ibid.
12. Ibid.
13. Downes, *The Laws of Disruption*, 272. ("Lawmakers have also too often heeded the siren call to do *something*, anything, to prove that digital life is not a lawless frontier," he says. "But legislating ahead of the technology helps no one and often leaves behind rules that trap those who were doing nothing wrong.")
14. Ibid., 60.
15. Marsali Hancock et al., "From Safety to Literacy: Digital Citizenship in the 21st Century," *Threshold Magazine* (Summer 2009): 4.
16. Anne Collier, "'Delete Day': Students Putting Messages That Matter Online," *NetFamilyNews.org*, May 6, 2011, http://www.netfamilynews.org/?p=30376.
17. Anne Collier, "From Users to Citizens: How to Make Digital Citizenship Relevant," *NetFamilyNews.org*, November 16, 2009, http://www.netfamilynews.org/2009/11/from-users-to-citizen-how-to-make.html; Larry Magid, "We Need to Rethink Online Safety," *Huffington Post*, January 22, 2010, www.huffingtonpost.com/larry-magid/we-need-to-rethink-online_b_433421.html; Nancy Willard, *Comprehensive Layered Approach to Address Digital Citizenship and Youth Risk Online* (Eugene, OR: Center for Safe & Responsible Internet Use, November 2008), http://csriu.org/PDFs/yrocomprehensiveapproach.pdf; ConnectSafely.org, *Online Safety 3.0: Empowering and Protecting Youth,* http://www.connectsafely.org/Commentaries-Staff/online-safety-30-empowering-and-protecting-youth.html.
18. Anne Collier, "A Definition of Digital Literacy & Citizenship," *NetFamilyNews.org*, September 15, 2009, www.netfamilynews.org/2009/09/definition-of-digital-literacy.html.
19. Larry Magid, "Digital Citizenship and Media Literacy Beat Tracking Laws and Monitoring," *SafeKids.com*, August 29, 2011, http://www.safekids.com/2011/08/29/digital-literacy-critical-thinking-accomplish-more-than-monitoring-tracking-laws.
20. Ibid.
21. See Adam Thierer, *Public Interest Comment on Federal Trade Commission Report, Protecting Consumer Privacy in an Era of Rapid Change* (Arlington, VA: Mercatus Center at George Mason University, 2011), 9, http://mercatus.org/sites/default/files/public-interest

-comment-on-protecting-consumer-privacy-do-not-track-proceeding.pdf. ("[S]ome companies appear to be competing on privacy....[O]ne company offers an Internet search service...as being... more privacy-sensitive....[I]n response to Google's decision to change its privacy policies...Microsoft encouraged consumers to switch to Microsoft's more privacy-protective products and services.")

22. OnGuard Online, http://www.onguardonline.gov.
23. See http://www.smokeybear.com and http://en.wikipedia.org/wiki/Smokey_the_Bear.
24. http://en.wikipedia.org/wiki/Woodsy_Owl.
25. http://mcgruff.org.
26. http://www.nhtsa.dot.gov/portal/site/nhtsa/menuitem.cda13865569778598fcb6010dba046a0.
27. Ira S. Rubinstein, "Regulating Privacy by Design," *Berkeley Technology Law Journal*, 26 (2011), 1409; Peter Schaar, "Privacy by Design," *Identity in the Information Society*, 3 (2010), 267.
28. Ann Cavoukian, "2011: The Decade of Privacy by Design Starts Now," *ITBusiness*, January 15, 2011, http://blogs.itbusiness.ca/2011/01/2011-the-decade-of-privacy-by-design-starts-now.
29. Ibid.
30. Alexandra Deschamps-Sonsino, "Designing Security into the Internet of Things," *GigaOm*, October 3, 2013, http://gigaom.com/2013/10/03/designing-security-into-the-internet-of-things.
31. Andrew Clearwater, "The Evolving Privacy Profession: Analysing History and Prospects," *Data Protection Law & Policy* (October 2013), 13. ("The outlook for privacy professionals has never been better. The growth of privacy challenges will continue to support the need for privacy expertise.")
32. Kenneth A. Bamberger and Deirdre K. Mulligan, "New Governance Chief Privacy Officers, and the Corporate Management of Information Privacy in the United States: An Initial Inquiry," *Law & Public Policy* 33, no. 477 (2011).
33. International Association for Privacy Professionals, "About the IAPP," https://www.privacyassociation.org/about_iapp.
34. Kenneth A. Bamberger and Deirdre K. Mulligan, "Privacy on the Books and on the Ground," *Stanford Law Review* 63 (2011): 260.
35. See generally Adam Thierer, *Parental Controls & Online Child Protection: A Survey of Tools and Methods* (Washington, DC: Progress & Freedom Foundation, 2009), http://www.pff.org/parentalcontrols.
36. Adam Thierer, "Achieving Internet Order without Law," *Forbes*, June 24, 2012, http://www.forbes.com/sites/adamthierer/2012/06/24/achieving-internet-order-without-law.
37. See generally Adam Thierer, "Can We Adapt to the Internet of Things?," *Privacy Perspectives*, IAPP, June 19, 2013, https://www

.privacyassociation.org/privacy_perspectives/post/can_we_adapt_to_the_internet_of_things.

38. Bamberger and Mulligan, "Privacy on the Books and on the Ground," 247.
39. Ibid.
40. Ibid.
41. Ibid.
42. Wildavsky, *Searching for Safety*, 183. ("Regulation, because it deals with the general rather than with the particular, necessarily results in forbidding some actions that might be beneficial. Regulators cannot devise specifications sufficiently broad to serve as guidelines for every contingency without also limiting some actions that might increase safety. Because regulation is anticipatory, regulators frequently guess wrong about which things are dangerous; therefore, they compensate by blanket prohibitions.")
43. Ithiel de Sola Pool, *Technologies of Freedom: On Free Speech in an Electronic Age* (Cambridge, MA: Harvard University Press, 1983), 231.
44. Richard Epstein, *Simple Rules for a Complex World* (Cambridge, MA: Harvard University Press, 1995).
45. Peter Fleischer, "Privacy-Litigation: Get Ready for an Avalanche in Europe," *Peter Fleischer: Privacy…?* (blog), October 26, 2012, http://peterfleischer.blogspot.com/2012/10/privacy-litigation-get-ready-for.html?m=1.
46. Ibid. ("Within hours of any newspaper headline [accurate or not] alleging any sort of privacy mistake, a race begins among privacy class action lawyers to find a plaintiff and file a class action. Most of these class actions are soon dismissed, or settled as nuisance suits, because most of them fail to be able to demonstrate any 'harm' from the alleged privacy breach. But a small percentage of privacy class actions do result in large transfers of money, first and foremost to the class action lawyers themselves, which is enough to keep the wheels of the litigation-machine turning.")
47. Antone Gonsalves, "Courts Widening View of Data Breach Damages, Lawyers Say," *CSO Online*, October 29, 2012, http://www.csoonline.com/article/720128/courts-widening-view-of-data-breach-damages-lawyers-say.
48. For example, in October 2012, the web analytics company KISSmetrics agreed to settle a class-action lawsuit associated with its use of "supercookies," which tracked users online without sufficient notice or choice being given beforehand. The firm agreed to pay each consumer who was part of the suit $2,500. See Wendy Davis, "KISSmetrics Settles Supercookies Lawsuit," *Online Media Daily*, October 19, 2012, http://www.mediapost.com/publications/article/185581/kissmetrics-settles-supercookies-lawsuit.html#ixzz2A306a5mq.

49. For example, see Va. Code Ann. § 18.2-130, Peeping or spying into dwelling or enclosure.
50. See J. Howard Beales III, "The FTC's Use of Unfairness Authority: Its Rise, Fall, and Resurrection," Federal Trade Commission, June 2003, http://www.ftc.gov/speeches/beales/unfair0603.shtm; J. Thomas Rosch, "Deceptive and Unfair Acts and Practices Principles: Evolution and Convergence," speech at the California State Bar, Los Angeles, CA, May 18, 2007, http://www.ftc.gov/speeches/rosch/070518evolutionandconvergence.pdf; Andrew Serwin, "The Federal Trade Commission and Privacy: Defining Enforcement and Encouraging the Adoption of Best Practices," *San Diego Law Review* 48 (Summer 2011).
51. 15 U.S.C. § 45(a).
52. Federal Trade Commission, *Policy Statement on Unfairness*, 104 F.T.C. 949, 1070 (1984), 15 U.S.C. § 45.
53. Ibid.
54. FTC, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers* (Washington, DC: Federal Trade Commission, 2012), i–ii, http://ftc.gov/os/2012/03/120326privacyreport.pdf.
55. See, for example, Health Insurance Portability and Accountability Act (HIPAA) of 1996, Pub. L. 104-191, 110 Stat. 1936 (1996).
56. See, for example, Truth in Lending Act, 15 U.S.C. §§ 1601-1667(f) (2006); Fair Credit Reporting Act of 1970, 15 U.S.C. §§ 1681-1681(u) (2006).
57. See, for example, Children's Online Privacy Protection Act (COPPA) of 1998, 15 U.S.C. § 6501 (2006).
58. Christopher Wolf, "Targeted Enforcement and Shared Lawmaking Authority as Catalysts for Data Protection" (BNA Privacy and Security Law Report, October 25, 2010), 3, http://www.justice.gov.il/NR/rdonlyres/8D438C53-82C8-4F25-99F8-E3039D40E4E4/26451/Consumer_WOLFDataProtectionandPrivacyCommissioners.pdf. ("At the state level, legislatures have become the proving grounds for new statutory approaches to privacy regulation. Some of these developments include the enactment of data security breach notification laws…as well as highly detailed data security laws, enacted largely in response to data breaches. This partnership has resulted in a set of robust standards for the protection of personal data.")
59. Thierer, *Parental Controls*, 19, 41–42.
60. Ibid., 22.
61. This section adapted from Thierer, "A Framework for Benefit-Cost Analysis," 1055–105.
62. Cass Sunstein, *Laws of Fear: Beyond the Precautionary Principle* (Cambridge, UK: Cambridge University Press, 2005), 46.
63. Ibid., 45–46.

64. See Susan E. Dudley and Jerry Brito, *Regulation: A Primer*, 2nd ed. (Arlington, VA: Mercatus Center at George Mason University, 2012), 97–98 ("The cost of a regulation is the opportunity cost—whatever desirable things society gives up in order to get the good things the regulation produces. The opportunity cost of alternative approaches is the appropriate measure of costs. This measure should reflect the benefits foregone when a particular action is selected and should include the change in consumer and producer surplus"); Jerry Ellig and Patrick A. McLaughlin, "The Quality and Use of Regulatory Analysis in 2008," *Risk Analysis* 32, no. 855 (2012).
65. See Richard B. Belzer, "Risk Assessment, Safety Assessment, and the Estimation of Regulatory Benefits," Mercatus Working Paper (Arlington, VA: Mercatus Center at George Mason University, 2012), 5, http://mercatus.org/publication/risk-assessment-safety-assessment-and-estimation-regulatory-benefits.
66. White House, Office of Information and Regulatory Affairs, *Regulatory Impact Analysis: A Primer* (2011), 2, http://www.whitehouse.gov/sites/default/files/omb/inforeg/regpol/circular-a-4_regulatory-impact-analysis-a-primer.pdf.
67. Ibid.
68. Ibid.
69. Ibid.
70. Ibid., 7.
71. Ibid., 2, 5.
72. Office of Information and Regulatory Affairs, *Regulatory Impact Analysis*, 3.
73. Ibid., 3–4.

# VI. CONCLUSION: IT'S ABOUT FREEDOM, PROGRESS, AND PROSPERITY

It should be clear now that the case for permissionless innovation is synonymous with the case for human freedom more generally.

Indeed, in making the case against the stasis mentality and precautionary principle–based policies, we can link dynamism and permissionless innovation to the expansion of cultural and economic freedom throughout history. There is a symbiotic relationship between freedom and progress. In his book, *History of the Idea of Progress*, Robert Nisbet wrote of those who adhere to "the belief that freedom is necessary to progress, and that the goal of progress, from [the] most distant past to the remote future, is ever-ascending realization of freedom."[1] That is the vision I have attempted to outline and defend here. Freedom, including technological freedom, is essential to achieving progress.

Few scholars better connected the dots between freedom and progress than F. A. Hayek and Karl Popper, two preeminent philosophers of history and politics of the 20th century. "Liberty is essential in order to leave room for the unforeseeable and the unpredictable," Hayek taught us. "[W]e want it because we have learned to expect from it the opportunity of realizing many of our aims. It is because every individual knows so little and, in particular, because we rarely know which of us knows best that we trust the independent and competitive efforts of many to induce the emergence of what we shall want when we see it."[2]

In a similar vein, Popper explained that "the human factor is the ultimately uncertain and wayward element in social life and in all social institutions. Indeed this is the element which ultimately cannot be completely controlled by institutions…for every attempt at controlling it completely must lead to tyranny; which means, to the omnipotence of the human factor—the whims of a few men, or even one."[3]

This has ramifications for public policy, obviously. "Despite his best intentions, the government planner will tend to live in the past, for only the past is sure and calculable," explained technology historian George Gilder.[4] "The most serious damage inflicted by excessive controls is the discouragement of innovation and entrepreneurship and the perpetuation of slightly laundered and government-approved obsolescence," he noted.[5]

It is vital that we embrace dynamism and leave a broad sphere for continued experimentation by individuals and organizations alike because freedom, broadly construed, is valuable in its own right—even if not all of the outcomes are optimal or equal. As Clay Shirky rightly noted in his 2008 book, *Here Comes Everybody*,

> This does not mean there will be no difficulties associated with our new capabilities—the defenders of freedom have long noted that free societies have problems peculiar to them. Instead, it assumes that the value of freedom outweighs the problems, not based on calculation of net value but because freedom is the right thing to want for society.[6]

The "value of freedom" is "the right thing to want for society" because it allows humans to grow, learn, prosper, and enjoy life. "Progress is movement for movement's sake," Hayek argued, "for it is in the process of learning, and in the effects of having learned something new, that man enjoys the gift of his intelligence."[7] Pessimistic critics will persist in their claims that our culture and economy can be guided down the proverbial "better path," but the path we're on right now isn't looking so bad and does not require the intrusive, freedom-crushing prescriptions that some critics call for.

Not everything will be sunshine and roses in a world of permissionless innovation. Mistakes will be made and there will even be short-term spells of what many would regard as particularly difficult social and cultural disruptions. *The crucial question is how much faith we should place in precautionary thinking and preemptive planning, as opposed to evolving social norms and ongoing trial-and-error experimentation, to solve those problems*.[8]

Those with an appreciation of liberty and the importance of trial-and-error experimentation will have more patience with technological change and be willing to see how things play out. This is rooted in our belief that social and economic disruptions are ultimately better addressed by voluntary, spontaneous, bottom-up responses than by coercive, top-down, centrally planned, technocratic approaches.[9]

The decisive advantage of the bottom-up approach is its nimbleness. It is during what some might regard as a market's darkest hour when some of the most exciting innovations and disruptive technologies emerge.[10] People don't sit still; they respond to incentives and suboptimal cultural and economic challenges. But they can only do so if they are truly free from artificial constraint from government forces that, inevitably, are always one or two steps behind fast-moving technological developments.

We shouldn't allow pessimistic techno-planners to sell us a version of "freedom" in which markets and cultural norms are constantly being reshaped and contorted through incessant regulatory interventions. That isn't true freedom; that's control. Permissionless innovation offers us a more promising, freedom-preserving, and progress-enhancing way forward.

Finally, if permissionless innovation advocates hope to triumph over precautionary principle thinking, it is essential that we avoid falling prey to what philosopher Michael Sacasas refers to as "the Borg Complex," which, he says, is often "exhibited by writers and pundits who explicitly assert or implicitly assume that resistance to technology is futile."[11] Indeed, some Pollyannaish pundits adopt a cavalier attitude about the

impact of technological change on individuals and society. That approach must be rejected.

Those of us who espouse the benefits of permissionless innovation must be mature enough to appreciate and address the occasional downsides of technological change. A "just get over it" attitude toward the challenges sometimes posed by technological change is never wise. In fact, it is downright insulting. We must instead listen to concerns about emerging technologies and offer constructive alternatives.

But we should also ask critics to think through the consequences of preemptively prohibiting technological innovation and to realize that not everyone shares the same values, especially pertaining to privacy, safety, and security issues. We should encourage them to avoid imposing their value judgments on everyone else by force of law and instead ask them to work with us to find practical, bottom-up solutions that will help individuals, institutions, and society learn how to better cope with technological change over time. Using this approach, we will have a better chance of convincing them that we can embrace our dynamic future together.

## NOTES

1. Robert Nisbet, *History of the Idea of Progress* (New Brunswick, NJ: Transaction Publishers, 1994), 236.
2. F. A. Hayek, *The Constitution of Liberty* (London: Routledge, 1960, 1990), 29.
3. Karl Popper, *The Poverty of Historicism* (London: Routledge, 1957, 2002), 146–7.
4. Gilder, *Wealth & Poverty: A New Edition for the 21st Century* (Washington, DC: Regnery Publishing, 2012), 329.
5. Gilder, *Wealth & Poverty*, 326.
6. Clay Shirky, *Here Comes Everybody: The Power of Organizing without Organizations* (New York: Penguin Press, 2008), 298.
7. Hayek, *The Constitution of Liberty*, 41.
8. It is what Postrel was referring to when she centered her dynamist vision around "the unpredictable, spontaneous, and ever shifting, a pattern created by millions of uncoordinated, independent decisions." See Postrel, *The Future and Its Enemies*, xv.

9. See Adam Thierer, "Our Conflict of Cyber-Visions," *Cato Unbound*, May 14, 2009, http://www.cato-unbound.org/2009/05/14/adam-thierer/our-conflict-cyber-visions.
10. See Jerry Ellig and Daniel Lin, "A Taxonomy of Dynamic Competition Theories," in *Dynamic Competition and Public Policy: Technology, Innovation, and Antitrust Issues*, ed. Jerry Ellig (Cambridge, UK: Cambridge University Press, 2001), 19. ("Schumpeterian competition is a dynamic vision. Because change requires time, the benefits of competition may not arrive immediately. Market participants may have to tolerate short-run inefficiencies in order to gain long-run efficiencies.")
11. Michael Sacasas, "Borg Complex: A Primer," *Frailest Thing*, March 1, 2013, http://thefrailestthing.com/2013/03/01/borg-complex-a-primer.

# ADDITIONAL READINGS BY ADAM THIERER

## JOURNAL ARTICLES AND BOOK CHAPTERS

- "Technopanics, Threat Inflation, and the Danger of an Information Technology Precautionary Principle," *Minnesota Journal of Law, Science & Technology*, 14 (2013): 309–86.
- "The Pursuit of Privacy in a World Where Information Control Is Failing," *Harvard Journal of Law & Public Policy*, 36 (2013): 409–55.
- "A Framework for Benefit-Cost Analysis in Digital Privacy Debates," *George Mason University Law Review*, 20, no. 4 (Summer 2013): 1055–105.
- "The Case for Internet Optimism, Part 1: Saving the Net from Its Detractors," in *The Next Digital Decade: Essays on the Future of the Internet*, ed. Berin Szoka and Adam Marcus (Washington, DC: Tech Freedom, 2010), 57–87.

## BLOG POSTS

- "Who Really Believes in 'Permissionless Innovation'?," *Technology Liberation Front*, March 4, 2013.
- "What Does It Mean to 'Have a Conversation' about a New Technology?," *Technology Liberation Front*, May 23, 2013.
- "Planning for Hypothetical Horribles in Tech Policy Debates," *Technology Liberation Front*, August 6, 2013.

- "On the Line between Technology Ethics vs. Technology Policy," *Technology Liberation Front*, August 1, 2013.
- "Edith Ramirez's 'Big Data' Speech: Privacy Concerns Prompt Precautionary Principle Thinking," *Technology Liberation Front*, August 29, 2013.
- "When It Comes to Information Control, Everybody Has a Pet Issue & Everyone Will Be Disappointed," *Technology Liberation Front*, April 29, 2011.
- "Copyright, Privacy, Property Rights & Information Control: Common Themes, Common Challenges," *Technology Liberation Front*, April 10, 2012.
- "Can We Adapt to the Internet of Things?," *IAPP Privacy Perspectives*, June 19, 2013.
- "Why Do We Always Sell the Next Generation Short?," *Forbes*, January 8, 2012.
- "The Six Things That Drive 'Technopanics,'" *Forbes*, March 4, 2012.
- "10 Things Our Kids Will Never Worry About Thanks to the Information Revolution," *Forbes*, December 18, 2011.
- "Achieving Internet Order without Law," *Forbes*, June 24, 2012.

### TESTIMONY / FILINGS

- Senate Testimony on Privacy, Data Collection & Do Not Track, April 24, 2013.
- Comments of the Mercatus Center to the FTC on Privacy and Security Implications of the Internet of Things, May 31, 2013.
- Comments of the Mercatus Center to FAA on commercial domestic drones (with Jerry Brito and Eli Dourado), April 23, 2013.

# ABOUT THE AUTHOR

Adam Thierer is a senior research fellow with the Technology Policy Program at the Mercatus Center at George Mason University. He specializes in technology, media, Internet, and free-speech policies, with a particular focus on online safety and digital privacy. His writings have appeared in the *Wall Street Journal*, the *Economist*, the *Washington Post*, the *Atlantic*, and *Forbes*, and he has appeared on national television and radio. Thierer is a frequent guest lecturer and has testified numerous times on Capitol Hill.

Thierer has authored or edited eight books on topics ranging from media regulation and child safety issues to the role of federalism in high-technology markets. He contributes to *Technology Liberation Front*, a leading tech policy blog.

Thierer has served on several distinguished online safety task forces, including Harvard University's Internet Safety Technical Task Force and the federal government's Online Safety Technology Working Group.

Previously, Thierer was president of the Progress & Freedom Foundation, director of telecommunications studies at the Cato Institute, and a senior fellow at the Heritage Foundation. Thierer received his MA in international business management and trade theory at the University of Maryland and his BA in journalism and political philosophy from Indiana University.