The Privacy Panic Cycle: A Guide to Public Fears About New Technologies

BY DANIEL CASTRO AND ALAN MCQUINN | SEPTEMBER 2015

Dire warnings about the privacy risks associated with new technologies routinely fail to materialize, yet because memories fade, the cycle of hysteria continues to repeat itself.

Innovative new technologies often arrive on waves of breathless marketing hype. They are frequently touted as "disruptive!", "revolutionary!", or "game-changing!" before businesses and consumers actually put them to practical use. The research and advisory firm Gartner has dubbed this phenomenon the "hype cycle." It is so common that many are conditioned to see right through it. But there is a corollary to the hype cycle for new technologies that is less well understood and far more pernicious. It is the cycle of panic that occurs when privacy advocates make outsized claims about the privacy risks associated with new technologies. Those claims then filter through the news media to policymakers and the public, causing frenzies of consternation before cooler heads prevail, people come to understand and appreciate innovative new products and services, and everyone moves on. Call it the "privacy panic cycle."

Dire warnings about the privacy risks associated with new technologies routinely fail to materialize, yet because memories fade, the cycle of hysteria continues to repeat itself. Unfortunately, the privacy panic cycle can have a detrimental effect on innovation. First, by alarming consumers, unwarranted privacy concerns can slow adoption of beneficial new technologies. For example, 7 out of 10 consumers said they would not use Google Glass, the now discontinued wearable head-mounted device, because of privacy concerns.[1] Second, overwrought privacy fears can lead to ill-conceived policy responses that either

purposely hinder or fail to adequately promote potentially beneficial technologies. For example, U.S. policymakers have delayed the adoption of various public sector technologies, from smart meters to electronic identification, in part because of the pushback these technologies have received from privacy advocates.[2]

This report describes the common trajectory of the privacy panic cycle and illustrates how inflated privacy concerns have played out for a number of well-known technologies. It looks at what causes the panic cycle and how certain factors have amplified the trend in recent years. Finally, it discusses the need for policymakers to understand this phenomenon so they do not mistakenly implement policies detrimental to innovation based on exaggerated fears.

UNCHECKED FEARS SLOW TECHNOLOGICAL PROGRESS

People have the tendency to fear the unknown and accept the commonplace. A "mass moral panic" occurs when one section of society distrusts or fears the choices made by others and believes these choices pose a risk to the society as a whole.[3] A "techno-panic" is an extension of this idea, and it occurs when a segment of society fears some aspect of technological change.[4] Often, the fears center on an anticipated problem that does not come to pass: at various points in time, people thought that reading novels could corrupt the "morals of many a promising youth"; that movies could make children lead "dissolute lives"; and that the telephone could make people lazy.[5] While society eventually overcomes techno-panics, they can significantly slow the pace of technological progress, imposing real costs on society in the process.

Today, consumers routinely use technologies that at one point some segment of society deeply distrusted, including telephones, toll roads, loyalty cards, cameras, RFID cards, and even computers. For example, when the Kodak portable camera was introduced in 1888, it quickly set off a panic over privacy concerns. People were horrified that tactless shutterbugs would take embarrassing photographs of them without their permission. Even President Theodore Roosevelt upbraided this use of the technology, telling a boy who tried to take his picture during his first week in office, "You ought to be ashamed of yourself."[6] Yet today most Americans carry pocket-sized devices with cameras everywhere they go and no one gives it a second thought.

THE PRIVACY PANIC CYCLE

Most people are willing to make tradeoffs between privacy and other values, such as convenience or cost-savings, but some are not. Those few—described by privacy researcher Alan Westin as privacy fundamentalists—often react viscerally to new technologies out of fear that they will result in diminished privacy.[7] As privacy fundamentalists speak out about their fears, these concerns creep into the public consciousness, and as they become widely discussed, they eventually reach a fever pitch. However, as people begin to use the technology, public understanding and appreciation of the technology grow and fears abate. Over time, public concern about the technology fades because most consumers realize their fears were misplaced, they use social norms to manage the technology, or they simply accept the tradeoffs since the benefits so vastly outweigh the cost or inconvenience. In the

end, only a small group of privacy fundamentalists continue to express privacy fears about the technology. This standard chain of events is the privacy panic cycle (figure 1).

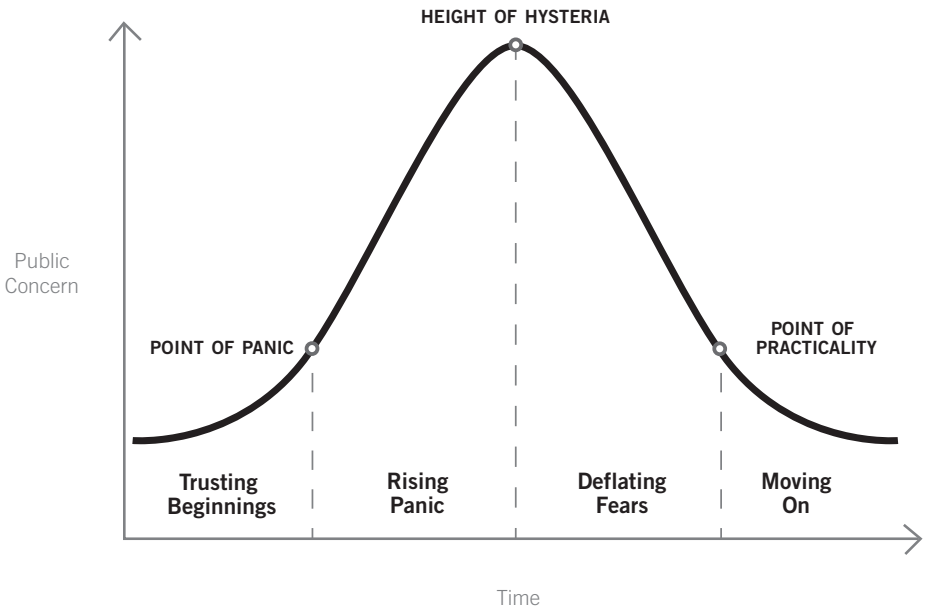

Figure 1: Privacy panic cycle.

As new technology starts to become more well-known, privacy fundamentalists—those individuals and organizations with deep commitments to privacy regardless of the costs—begin to raise alarms.

The privacy panic cycle describes the recurring pattern of privacy fears that appear following the introduction of a new technology. It charts how perceived privacy fears about a technology grow rapidly at the beginning, but eventually decline over time. The privacy panic cycle is divided into four stages: Trusting Beginnings, Rising Panic, Deflating Fears, and Moving On. A number of different factors affect the duration and intensity of the privacy panic cycle, and these will be discussed in the next section of the report.

Stage 1: Trusting Beginnings

The privacy panic cycle starts with the invention of a new technology. In the beginning, only a core group of people have knowledge of a new technology. This group consists of the inventors and innovators (the engineers and designers who are developing the technology and beginning to commercialize it) and the "technorati" (people who closely follow new technological developments). During this period, the technology has not yet been widely deployed and privacy concerns are minimal.

As the technology starts to become more well-known outside of this relatively small circle, privacy fundamentalists—those individuals and organizations with deep commitments to privacy regardless of the costs—begin to raise alarms about the technology. These claims are often hyperbolic or simply misleading. For example, Brad Templeton, the chairman of the Electronic Frontier Foundation (EFF), made a presentation about the "evils of cloud computing" at a technology conference in 2009 where he admitted that many in the audience likely knew nothing about the technology.[8] Similarly, the organization Consumers Against Supermarket Privacy Invasion and Numbering (CASPIAN) described radio frequency identification technology (RFID) as a technology much more powerful than is actually the case, and as a harbinger of a dystopian future.[9] The public, not yet

familiar with the technology, takes these claims at face value and panic begins. This marks the "Point of Panic" and the end of the initial stage.

Stage 2: Rising Panic

Once privacy fundamentalists succeed in drawing negative attention to a technology, others start fanning the flames of fear, either intentionally or unintentionally. This includes the media who want to advance popular stories; politicians in search of hot issues to attract voters; government regulators trying to maintain or gain relevancy; and researchers seeking to advance their academic careers by becoming more well-known. Fear makes for excellent click-bait, and as these groups try to promote their own self-interest by repeating the claims of privacy fundamentalists and speaking out against the technology, they spread fear among consumers. This stage is the Rising Panic stage.

Many individuals and organizations jump on the bandwagon during this stage, knowing that making outrageous claims about privacy are a sure path to recognition. As a result, the public often hears overblown fears with a false sense of urgency. Because of the crowded field, the media tends to recognize those with the most outrageous claims, setting a pattern whereby it continuously escalates the perceived implications, challenges, and threats brought by the technology.[10] Privacy fundamentalists spew hyperbolic and emotional rhetoric that the media then repeats and amplifies. This stage has given rise to apocalyptic and dystopian imagery for new technologies such as those invoking a "privacy Chernobyl," "Big Brother," "the Mark of the Beast," and "Stalkers, Inc." (figure 2).[11]

Figure 2: Privacy imagery used to scare consumers.[12]

Policymakers then pick up these concerns, especially elected officials looking for issues with popular appeal, and then repeat the same rhetoric as the privacy fundamentalists. Whether through investigations, committee hearings, stakeholder groups, floor speeches, or on-camera interviews, these officials further elevate unreasonable privacy concerns. Likewise, regulators often enthusiastically join the cycle, holding hearings, issuing reports, and giving speeches, all warning that without their vigilant protection a privacy Armageddon is just around the corner. These actions further feed the media frenzy, and consumers' fears continue to rise.

During Rising Panic, consumers are just beginning to understand the technology and its benefits, making them more susceptible to false statements. In most cases, because they have not had direct experience with the technology, privacy fundamentalists can make virtually any claim about the technology without losing credibility. For example, RFID opponents suffered little loss of reputation for routinely making false claims about the technology, such as that the RFID tags typically used in supply chain management could be read from 30 feet away.[13]

In most cases, because consumers have not had direct experience with the technology, privacy fundamentalists can make virtually any claim without losing credibility.

Privacy fears continue to climb until public understanding about the technology and its benefits reaches a tipping point. Various external factors, such as changes in the level of adoption and use of the technology, or disillusionment when fears never materialize, can affect when this tipping point occurs. At the end of the Rising Panic stage, privacy fears reach their zenith at the Height of Hysteria.

Stage 3: Deflating Fears

Eventually the public dismisses the privacy concerns associated with the technology. This occurs as the technology becomes increasingly commonplace and interwoven into society. This stage is called Deflating Fears, and it represents the period during which the general public comes to embrace the technology and privacy concerns decline.

During Deflating Fears, new events may cause micro-panics—smaller panics that myopically focus on the privacy concerns of one aspect of the technology or its integration into society. For example, a new feature of a technology might generate renewed privacy fears. These micro-panics push privacy concerns back to the forefront of public attention through media buzz. However, the micro-panics quickly disappear or are forgotten about. For example, while the Height of Hysteria for RFID technologies peaked in 2007, the issue was brought to the forefront again in 2012 when a school in Texas implemented mandatory RFID chips in its students' ID badges.[14] One student took issue with this policy, and citing religious and privacy concerns, took the school to court. Despite the fact that this episode succeeded in capturing the media spotlight for a few weeks, the story quickly faded and consumer concern with RFID dissipated once again. These micro-panics do not significantly impact the overall privacy panic cycle of the technology, but show that at least some privacy fundamentalists continue to incite privacy fears even after the majority of the population has moved on.

The third stage of the privacy panic cycle ends with the Point of Practicality, where illusory privacy concerns have faded. At this point, the majority of the general public no longer

believes the privacy claims made by privacy fundamentalists, and the technology has reached a sufficient level of maturity that most people no longer express concerns about its misuse. The technology is just part of life.

Stage 4: Moving On

In the final stage of the privacy panic cycle, the vast majority of consumers no longer believe the privacy claims espoused by the privacy fundamentalists because they understand the technology, appreciate its benefits, and no longer fear its misuse. While there may be some lingering concerns with the technology, they are far more muted, and they are likely to be addressed with level-headed policy interventions.

For example, some web-based email providers display personalized ads based on automated analysis of the content of users' email messages.[15] When Google first rolled out this feature for its Gmail service in 2004, over 30 privacy-focused organizations wrote to the company asking it to suspend the service until it addressed all of their privacy complaints.[16] But as its email service quickly become popular with tens of millions of consumers despite these complaints, lawmakers and regulators did not intervene. Instead, they later began to review general issues with privacy for users of cloud-based email services, such as different standards for law enforcement access, and have proposed reasonable updates to the Electronic Communications Privacy Act (ECPA).[17]

However, even in this final stage, privacy fundamentalists still raise privacy concerns with technologies, whether or not they are valid. But most organizations focused on privacy recognize that if they are to stay relevant, especially to donors, they must find new "products" for the next privacy panic cycle. For example, CASPIAN only moved on to RFID after its initial efforts to oppose supermarket loyalty cards, which most consumers readily accepted, fell short.[18]

As new technologies emerge, the panic cycle is likely to begin anew. For example, while the portable camera was built in the late 1800s, developments to the technology—such embedding cameras in cell phones or in wearable technology—elicited a new privacy panic cycle.[19]

FACTORS INFLUENCING THE PRIVACY PANIC CYCLE

From the introduction of satellites to the dawning of the Internet, many technologies have gone through privacy panic cycles of varying lengths and intensities. There are a number of factors that affect the privacy panic cycle of a particular technology, including:

- The level of technological obscurity
- The level of trust in the producers or users of the technology
- The perceived value of the technology

Level of Technological Obscurity

Consumers are more likely to fear technologies that they are less familiar with.[20] It is easier for privacy fundamentalists to create hyperbolic or false concerns about technologies that the public has had little exposure to. For example, since most people do not know how

GPS works, they may believe the false claim that it can be used to track individuals in real-time, even though it is not capable of transmitting location data, only of receiving it.[21] When most people do not understand how a particular technology works, it is easy for privacy fundamentalists to exacerbate privacy fear.

The rate at which consumers adopt a technology also affects the length of the privacy panic cycle. Technology adoption breeds public familiarity with the technology, which, in turn, decreases the obscurity of the technology and shortens the privacy panic cycle of that technology. Sometimes, however, policymakers introduce laws or regulations limiting the deployment of new technologies and thus lengthening the duration of the privacy panic cycle.

If a technology offers a clear social good, then people are less likely to demonize it, although that by no means stops privacy fundamentalists from trying.

Level of Trust in the Producers or Users of the Technology

Consumers' fears about technology are exacerbated when the technology is produced or used by organizations they distrust. For example, when the U.S. government rolled out the ineptly named program Total Information Awareness—a data-mining program intended to gather commercial information to prevent threats to national security—it was defunded by Congress due to large public outcry generated by privacy fundamentalists.[22] Similarly, large iconic companies like Google and Facebook usually become a lightning rod for privacy controversy, with privacy fundamentalists crying foul over almost every new feature they introduce.[23]

Distrust of government has stalled the progress of many technologies. For example, unwarranted fears that government will begin tracking motorists have derailed efforts to implement vehicle miles traveled (VMT) taxes, a tax system that charges drivers fees based on the amount they drive rather than on the amount of gasoline they purchase, even though VMT technology would only report payment information and share no data about a driver's movements.[24]

The Perceived Value of the Technology

If the public recognizes that a new technology offers a lot of public value or consumer benefits, the privacy panic cycle for that technology may be short. For example, consumers quickly adopted mobile phones in spite of some privacy concerns because of the clear benefits these devices offered. This is despite the fact that by virtue of the technology, wireless carriers can triangulate the location of any subscriber. Likewise, when it came to e-commerce, many people were initially hesitant to enter their credit card information into a computer.[25] However, this practice spread quickly when people realized the benefits of e-commerce and understood that the risk of credit card misuse is actually lower online than off.

If a technology offers a clear social good, then people are also less likely to demonize it, although that by no means stops privacy fundamentalists from trying. For example, police body-cameras present a privacy challenge because they record each interaction that an officer has with civilians. For many years, privacy advocates resisted this technology. However, given the recent rise in awareness of police abuse, citizens are much more open to using this technology to increase accountability in U.S. law enforcement.[26] Policymakers

from both sides of the aisle have now endorsed this strategy as a means to reform police institutions and build public trust.[27]

TRENDS INFLUENCING THE PRIVACY PANIC CYCLE

Over time the privacy panic cycle has gotten more intense for all technologies as major factors have shaped society. There are a number of trends that have made the privacy panic cycle more volatile over time. These factors include:

- The Internet and social media
- Privacy professionals
- Privacy-focused companies
- The news media
- Privacy advocacy groups

The Internet and Social Media

The Internet, especially blogs and social media, has given more people a platform to share their unfiltered opinions. Information is free to flow not only between mainstream media outlets and the public, but also among bloggers, citizen journalists, online talking heads, peers on social media, and other sources. This free exchange allows information about new technologies and peoples' reactions to those technologies to percolate through society at a faster rate than before.

Furthermore, the Internet has made it easier to spread misinformation. Many websites, citizen journalists, and blogs post unverified information. For example, one blog passed around the idea that the Affordable Care Act, often referred to as Obamacare, was going to force all U.S. citizens to be tagged with a chip to track them.[28] Other media websites discredited this information, but not before the post had almost 300,000 views and over 101,000 likes on Facebook.[29] The story had originated from a satirical news website, called the *National Report*, which the blogs had taken seriously.[30] The Internet has also allowed for groups to coalesce around ideas more easily. This has allowed groups like CASPIAN or the EFF to spread dubious information while growing their membership base.[31]

Privacy Professionals

Led by organizations such as the International Association of Privacy Professionals, there is now a professional class of people whose job is to manage privacy risks and promote the idea that technology is becoming more invasive.[32] These privacy professionals have a vested interest in inflating the perceived privacy risk of new technologies as their livelihood depends on businesses' willingness to pay them to address these concerns. As with other organized labor associations, their views often play an outsized role in policy and politics.

Privacy-Focused Companies

Many companies—from small start-ups to large tech giants—have begun selling products and services to capitalize on consumer privacy concerns. For example, one privacy lawyer-turned-entrepreneur launched a company to sell TrackOFF, software designed to allay Internet users' fears about surreptitious online tracking, while other companies sell products designed to obscure license plates from red-light cameras.[33] Because these

companies have a vested interest in selling privacy protections, their efforts to grow their businesses feed the privacy panic cycle. Venture capitalists have begun investing heavily in some of these businesses, creating a strong financial incentive to continue overstating privacy concerns.[34]

The News Media

Media companies, including newspapers, magazines, and other publishers, have a symbiotic relationship with privacy advocates since doomsday predictions make for good headlines. Some have even gone so far as to become part of the story by hiring privacy advocates to generate the stories that their editors publish.[35] Ironically, such "investigative reporting" often turns up criticism that applies even to the parent company of these publishers.[36]

In addition, in today's fast-paced, highly competitive media environment, many publishers go with headlines that stand out, regardless of their merits. So rather than simply have a story about an advocacy group that is pushing a particular perspective, a publisher will put out a headline like "Everything is watching YOU."[37] Any nuance is completely lost in the headline, which may be the only thing many people see in their social media feed.

Privacy Advocacy Groups

The number of advocacy groups focused on privacy issues has grown significantly in recent years (figure 3). Some of these advocacy groups have an incentive to find cause for alarm, even where none might exist, and to raise consumer privacy fears in order to attract additional funding and validate their mission.[38] Others exaggerate privacy concerns in an effort to pressure companies to agree to pay a settlement in class action lawsuits brought against them—payments that may go to privacy advocacy organizations. For example, the Electronic Frontier Foundation and the Center for Democracy and Technology each received half a million dollars as a result of a class action settlement with Facebook concerning the privacy implications of one of its features.[39]

Privacy Advocacy Groups	Year Founded
Electronic Frontier Foundation	1990
Privacy International	1990
Privacy Rights Clearinghouse	1992
Electronic Privacy Information Center	1994
Center for Democracy and Technology	1994
Consumers Against Supermarket Privacy Invasion and Numbering (CASPIAN)	1999
International Association of Privacy Professionals	2000
Center for Digital Democracy	2001

Common Sense Media	2003
Patient Privacy Rights	2004
Future of Privacy Forum	2008
Georgetown Center on Privacy and Technology	2014

Figure 3: U.S.-based privacy advocacy groups founded since 1990.

THE PRIVACY PANIC CYCLE IN ACTION

The privacy panic cycle applies to many technologies, new and old. Examining the historical record makes clear that privacy concerns about technology are not new, and that these concerns generally dissipate over time without the need for policymakers to intervene.

Portable Cameras

In addition to having inspired many modern concepts about privacy, the portable camera provides a notable example of the privacy panic cycle.[40] In 1888, George Eastman invented the Kodak camera, the original portable camera.[41] Unlike with other cameras at the time, subjects no longer had to maintain a pose for upwards of one minute.[42] This small, hand-held contraption cost $25, a large amount of money at that time, but still less than the cost of the older wet-plate cameras.[43] It offered simplicity and reliability. The camera came with 100 shots preinstalled. When the owner was done he or she could ship the entire camera back to the factory and the company would reload it and send it back.[44] This was summarized in the original Kodak slogan: "You press the button, we do the rest."[45] This was the start of the Kodak camera's Trusting Beginnings stage.

Figure 4: Kodak camera advertisement in 1889[46]

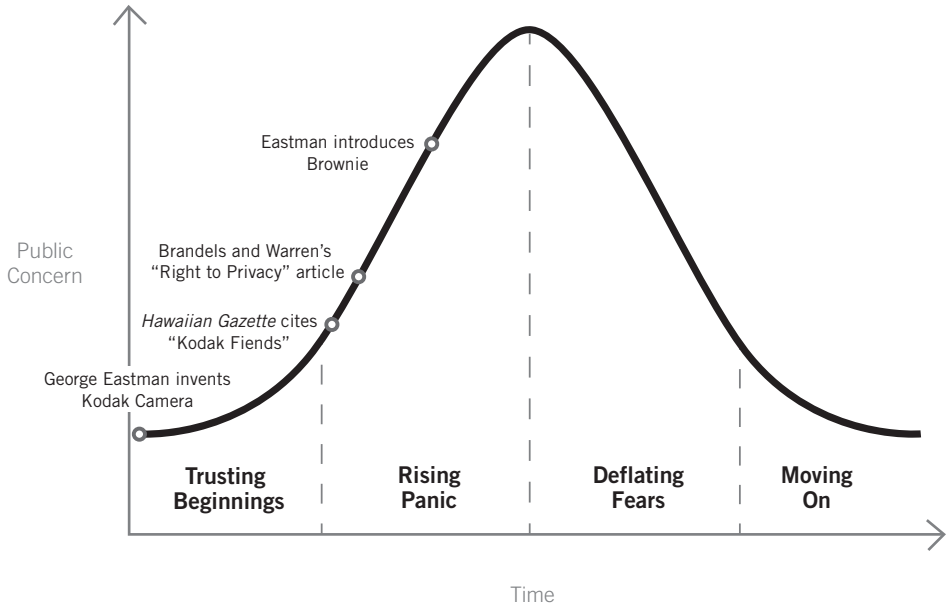

Figure 5: The privacy panic cycle of the portable camera.

With the introduction of the portable camera, suddenly photography was everywhere. People took their cameras outside to parks, beaches, and fairs. These amateur photographers were captivated by the newfound ability to capture everyday motion, candid photos, and "snap shots." Because of the relatively low price, convenience, and simplicity of the Kodak, photography became a fixture of American culture, leading the *Chicago Tribune* to proclaim in 1897, "The craze is spreadin g fearfully. Chicago has had many fads whose careers have been brilliant but brief. But when amateur photography came, it came to stay."[47] The Kodak camera's ease of use and large adoption rates sped it through the privacy panic cycle in a rapid manner.

Not everyone saw the benefits of this innovation, and as it began to become more popular, privacy fundamentalists raised alarms about the technology. With so many people carrying around cameras, people became concerned that their picture would be taken without permission. The media grabbed hold of this fear. In the summer of 1888, one newspaper, the *Hartford Courant*, wrote the following: "Beware the Kodak. The sedate citizen can't indulge in any hilariousness without the risk of being caught in the act and having his photograph passed around among his Sunday school children."[48] Suddenly, people feared that cameras threatened their privacy and reputation. By 1890 this technology had moved to its Rising Panic stage.

Privacy fundamentalists, buoyed by newspapers of the day, built up the idea of the "Kodak fiend," a person who took unflattering pictures or pictures without permission.[49] The *Hawaiian Gazette* described the Kodak fiend this way:

> *"Have you seen the Kodak fiend? Well, he has seen you. He caught your expression yesterday while you were in recently talking at the Post Office. He has taken you at a disadvantage and transfixed your uncouth position and passed it on to be laughed at by*

> *friend and foe alike. His click is heard on every hand. He is merciless and omnipresent and has as little conscience and respect for proprieties as the verist hoodlum. What with Kodak fiends and phonographs and electric search lights, modern inventive genius is certainly doing its level best to lay us all bare to the gaze of our fellow men."*[50]

The *New York Times* wrote of Kodak fiends snapping pictures of women without their permission and of threats made against those who used their cameras too freely.[51] Local governments and businesses subsequently banned Kodak cameras at beaches and other outdoor spaces. One beach resort feared the Kodak fiend so much it posted the notice, "People are forbidden to use their Kodaks on the beach."[52] In fact, one journalist described a situation in which young men in Britain formed a "Vigilance Association" with the sole purpose of "thrashing the cads with cameras who go about at seaside places taking snapshots of ladies emerging from the deep."[53] The portable camera was also banned from the Washington Monument.[54] Indeed, these privacy concerns continued to ramp up to a fever pitch over the next decade as the technology grew in popular use.

Then in 1900, Eastman created the next camera installment, the Brownie, a camera that only cost $1, and rolls of film that were only $0.15 each.[55] Within the first year, Eastman sold 150,000 Brownie cameras. In fact, sales were so high that by 1905 a third of American households owned some sort of camera.[56] With the increased use of the Brownie came another invention, the postcard. With the enhancement of printing techniques and economies of scale brought by cheaper cameras, postcards decreased in cost from two cents to one, and became incredibly popular. For example, on a single day in September 1906, an astonishing 200,000 postcards were postmarked from Coney Island alone.[57] This increased and wide-spread use of the technology helped acclimatize the public to its popular use. By 1910, the portable camera's privacy panic cycle had moved on past the Height of Hysteria towards its Deflating Fears stage, as increasing numbers of people used the technology and grew to appreciate its benefits.

Undoubtedly, the privacy fears of the portable camera existed long after the Kodak's privacy panic cycle moved past its Point of Practicality into the Moving On stage, but these incidents were relatively rare.[58] These fears ultimately subsided as new cameras were invented. Today, all but a small fringe of consumers worry about the privacy implications of basic handheld cameras. Of course as companies create new camera technologies or embed cameras in new devices, such as wearable devices or cell phones, the privacy panic cycle revives.

Transistors

In the late 1940s, a group of Bell Lab employees invented the transistor—a key technological advancement that set the stage for the modern computing era. Over the next decade, the transistor existed in its Trusting Beginnings stage, where the technology was not yet widely used or known. Indeed noted privacy researcher Alan Westin observed that the 15 years after World War II saw little development in information technology and high public trust in government and businesses.[59]

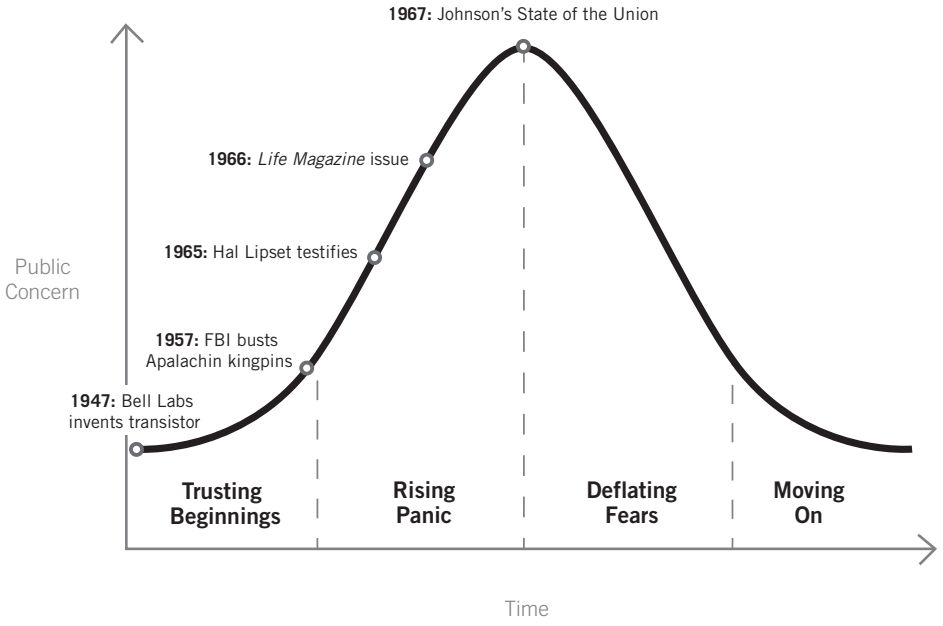

Figure 6: The privacy panic cycle of the transistor.

However, while the transistor became the building block for the modern day microchip, it also enabled electronic eavesdropping. Without the transistor and the printed circuit, miniaturization would not have been possible, and with it came the invention of the "bug"—miniaturized microphones used to record someone's conversation without their knowledge. Privacy fundamentalists cried foul, anticipating wide-spread abuse. As transistor manufacturing got better, the technology got smaller and privacy concerns swelled.

By the late 1950s, the transistor was in the Rising Panic stage. At the time, much of that decade's hysteria over national security threats had dwindled, but it was quickly replaced by a growing fear of organized crime. In 1957, federal investigators used surveillance to uncover a gathering of organized crime kingpins in Apalachin, New York. This subsequent news coverage raised awareness not only about crime syndicates, but also about snooping from transistor-enabled technologies, which in turn elevated fears about these devices in the national consciousness.

The "bug in the martini" took this fear to a new level. When Hal Lipset, a private detective from San Francisco, testified before a U.S. Senate subcommittee in 1959 on these issues, he decided to use miniature transistor technology as a gimmick to showcase the surreptitiousness of budding devices. Lipset hid a recording device prior to his testimony, which he used to record the hearing. He then played it back for the senators. The senators disliked the stunt, believing it was proof that private electronic snooping had gotten out of hand, both because of improvements to the technology and because of the lack of prosecutions associated with illegal snooping under weak privacy laws at the time.[60] This further perpetuated a privacy uproar aimed at this technology.

Sen. Edward Long (D-MI), chairman of the Senate Judiciary Subcommittee on Administrative Practice, called a hearing in 1965 to discuss bugging technologies and invited Lipset to testify. The senator believed the best solution to bugging was a law requiring licensing of all bugging equipment, and called the hearing to justify his proposed privacy law.[61] This time Lipset alerted the senator's staff in advance of his intentions to make a dramatic gesture, and the staff encouraged him to do something to gin up headlines.[62] So Lipset hid a bug in a fake olive plopped inside an empty cocktail glass (no liquid could be used or the device would have short-circuited). In the hearing, Sen. Long played along with Lipset as he demonstrated a bug in the flowers left on the senator's desk and the olive in the martini glass. Cameras from national newspapers and television news stations captured the performance, elevating these false privacy concerns to their peak.

The rest of the hearing devolved into a discussion about the martini olive, as senators kept referring to it and asking questions about it. Lipset saw the senators' reaction and romanticized the idea, talking about bug variants disguised as lemon peels or onions instead of olives. No one seemed to notice how impractical it was; the oversized antenna masquerading as a toothpick had a limited range and the microphone would not work if there was any liquid in the glass. However, the gimmick succeeded in capturing national attention as the "bug in the martini" became a common reference point for the loss of privacy to inconspicuous bugging devices.

Figure 7: *Life* magazine from May 1966, which included an image of a bug in a martini.[63]

The press readily fed this hysteria. In May 1966, *Life* magazine—the most widely circulated magazine of the time—published an issue with a full-color picture of a woman pulling back her dress to reveal a transmitter taped to her back (figure 7).[64] The

implications of this issue were that ordinary citizens were conducting illegal surveillance of one another more than ever before. While *Life* reported that any surveillance by law enforcement could help their work, the magazine had something different to say about access to this technology by ordinary citizens:

> *"That justification does not exist for the growing legions of private citizens—businessmen, union officials, employers, suspicious spouses—who find it ridiculously easy to indulge in electronic spying. They can choose from a vast array of inexpensive, easy-to-install snooping devices which can be bought over the counter with no questions asked."* [65]

The issue focused on the myriad of ways citizens could spy on each other. *Life* published several 11-inch colored photographs of devices, including one of a tiny transmitter inside of fake plastic olive inside a cocktail glass with a clear liquid in it—further perpetuating the myth. The caption on the photo read, "Plopped in a martini, it can transmit cocktail party conversation 100 feet."[66] In the end, the hysteria was driven by fears not facts. *Life*'s proposition that "legions of private citizens" would start using illegal electronic surveillance never materialized.

Nevertheless, privacy concerns against transistor-enabled electronic surveillance ramped up to a fever pitch, and by 1967 the privacy panic cycle for this technology had hit its Height of Hysteria. In January of 1967, President Johnson mentioned the right to privacy in his State of the Union address saying, "We should outlaw all wiretapping, public and private… except when the security of the nation itself is at stake and only with the strictest of safeguards."[67]

The public's fears of transistors as a serious threat to privacy waned as they came to understand the technology. As privacy concerns declined, the zeal for legislation died. Sen. Long subsequently lost his 1968 reelection bid, calling his defeat a "victory for the wiretapper, snooper, and federal bureaucrat" who invades the privacy of ordinary citizens.[68] In his last year of office, Johnson signed into law a sweeping wiretapping legislation that spelled out rules for how the government could use electronic surveillance, including the use of bugs. The 1968 law also made it a federal crime to manufacture, distribute, possess, advertise, sell, or ship any electronic devices that would be primarily used for surreptitiously monitoring conversations. Johnson did not like signing the bill, doing so only because elements in it had been suggested by his administration due to the assassinations of Martin Luther King Jr. and Senator Robert F. Kennedy in 1968.[69] In fact, while he signed the bill into law, Johnson grumbled to himself that the bill would help confine "wiretapping and eavesdropping to national security cases only—and then only with the approval of the Attorney General."[70]

While the "bug in the martini" became a catchphrase in the 1970s for the unconstrained ability to listen to conversations by nefarious individuals, the focus of the population on transistor-enabled bugs continued to decrease.[71] By the 1980s, this technology was in its Moving On stage and most people had no privacy concerns about bugs, but rather about

other newer technologies. The privacy fundamentalists had moved to other technologies, and the bug in the martini was relegated to the dustbin of history.

Radio Frequency Identification (RFID) Tags

Radio frequency identification (RFID) tags began with a single shade of lipstick. When Procter & Gamble launched Oil of Olay's ColorMoist Hazelnut No. 650 in 1997, the dark-red lipstick was extremely popular.[72] Four in ten stores that carried this product rapidly sold out and P&G realized it needed a more efficient means to keep the lipstick in stock. In response, Kevin Ashton—a young brand manager in charge of the new product—attempted to find a means of tracking items through the supply chain so that store managers knew when to replenish their shelves.[73] Ashton soon identified RFID as a possible solution to this problem and reached out to two Massachusetts Institute of Technology (MIT) professors, Sanjay Sarma and David Brock, to test his hypothesis. These three invented a system in which each product was identified using an RFID tag with a unique 96-bit code, or Electronic Product Code (EPC), as well as a machine, called a reader, which could identify each tag individually. Until suppliers began placing RFID tags on consumer goods, RFID avoided public controversy and stayed in its Trusting Beginnings stage through the early 2000s.[74]

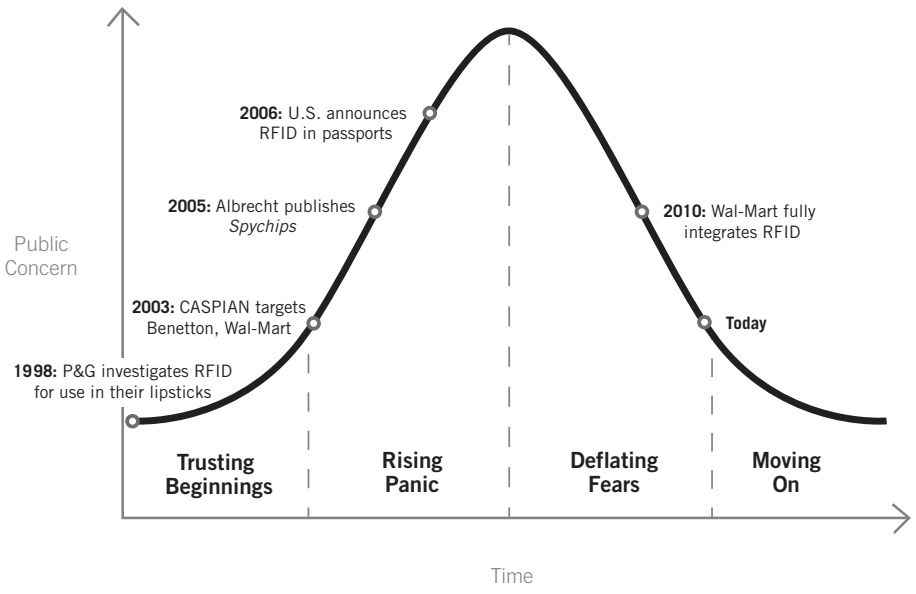

Figure 8: The privacy panic cycle of RFID.

By 2003, more than 100 companies had joined MIT's Auto-ID Center to pursue the integration of low-cost RFID tags on all products in order to track them through the supply chain. At the time, these retail giants and manufacturers were losing billions of dollars a year to lost or stolen items.[75] For example, at the time Gillette's razor blades were one of the most commonly stolen items.[76] The problem was not the shoplifter who pocketed a package of razors from the store, but rather the theft of large quantities of razors from within the company's supply chain. By tracking individual packages, RFID

technologies help maximize the level of visibility that companies have in their supply chains so that they can hold each part of the chain accountable, catching and reducing bulk theft.[77] As the private sector widely started to contemplate using this new technology, concerns driven by loss of privacy and paranoia from the general public started to rise. Some of the most outspoken critics famously referred to RFID chips worn on a person to be the "Mark of the Beast" from the Book of Revelation in the Bible.[78]

By 2002, the Rising Panic stage started for RFID as privacy advocacy groups seized upon the privacy concerns surrounding the new technology, and started broadcasting fears of its abuse. The Consumers Against Supermarket Privacy Invasion and Numbering (CASPIAN) consumer-rights group, which was founded in 1999 by Katherine Albrecht, a consumer privacy advocate, to protest supermarket loyalty card programs, took up the mantle of combating the roll out of RFID chips. In Albrecht's version of a dystopian future, a grocery store could scan a consumer's credit card when he or she entered the store (from within his or her bag), and track the consumer's movements and purchases throughout in the store.[79] This information would then find its way into "big brother" government hands.[80] Albrecht also seized onto and perpetuated the apocalyptic claims for RFID, claiming that this technology had "biblical implications."[81] Albrecht published several books to dissuade the adoption of RFID technologies.[82] One book, *Spychips,* presented a dystopian future in which corporations and governments created a "master plan" where hidden RFID readers were placed around stores and the community, tracking every purchase and by association every person. And the media helped perpetuate these ridiculous claims. Over the next decade, Albrecht would be cited in articles in the *New York Times*, the *Washington Post*, the *Wall Street Journal*, *Time* magazine, *Salon*, *CNN*, the *BBC*, and many more, and asked to write about privacy for mainstream magazines like *Scientific American*.[83]

Some of the most outspoken critics said that RFID chips worn on a person were the "Mark of the Beast" from the Book of Revelation.

The first major privacy concern pushed by privacy fundamentalists was the belief that the retail industry would abuse this technology on a large scale. CASPIAN believed that if a retailer would put RFID tags on every good, especially clothing, then it would use these tags to track not only purchases, but also individual movements. During its campaign, CASPIAN took on a number of large retail and supermarket stores. In 2003, CASPIAN and other privacy advocates pressured Italian retailer Benetton (BNG) into rescinding its trial of RFID when the company announced plans to embed RFID tags in its Sisley line of women's clothing.[84] Then, in a similar effort, CASPIAN went on to protest the plan of a Wal-Mart store in Brockton, Massachusetts to widely roll out RFID in its stores after it tested smart shelves at one of its locations. The campaign worked, and Wal-Mart would not fully deploy RFID until nearly seven years later.[85] CASPIAN was effective, in part, because consumers at the time knew little about RFID technology. A 2004 survey of more than 1,000 U.S. adults found that only 23 percent of respondents had heard of the technology.[86] Moreover, 40 percent of respondents feared that RFID tags could be read from afar, despite this not being technically possible.[87] In 2005, CASPIAN launched a worldwide plan to boycott Tesco, the multinational grocery and general merchandise retailer, over concerns related to the store's increasing use of RFID.[88] Tesco had also planned to explore tagging individual items with the technology.[89] In 2006, CASPIAN then targeted Levi Strauss & Company when it planned a trial using RFID tags clipped to the outside of the garment to focus on inventory management.[90]

CASPIAN also raised the concern that the government would mandate microchip implants in humans to track their movements. This would then lead to a surveillance society where, according to Albrecht, "networked RFID readers called 'person tracking units' would be incorporated virtually everywhere people go–in 'shopping malls, airports, train stations, bus stations, elevators, trains, airplanes, restrooms, sports arenas, libraries, theaters, [and] museums'—to closely monitor people's movements."[91] The hysteria caught on, and soon politicians and the media were repeating these claims. Bolstered by privacy advocates, several states—including California, North Dakota, Wisconsin, and Washington—passed laws banning coerced chip implants.[92] However, chip implants were rare and optional. In one well-known example, a bar offered a customer loyalty program where patrons could have a chip around the size of a grain of rice implanted in their arms, as a "fraud-proof" way to pay their tab.[93] In another example, a Florida family had tags containing their complete medical histories implanted under their skin to ensure "health security."[94] Both of these stories made headlines and elicited slippery-slope arguments from privacy advocates, but neither case involved the government and the implants did not allow the individuals involved to be tracked in either case.

During the Rising Panic, attempts by the government to use the technology caught the public eye. When the International Civil Aviation Organisation (ICAO) outlined plans in 2004 to create an international "identity register" that would standardize the use of RFID technology in all government-issued passports by 2015, 39 civil liberties groups, including CASPIAN, the EFF, and the ACLU, sent a letter to the organization opposing the plan.[95] In 2006, the United States complied with the ICAO's standards, rolling out an initiative where all new passports would be equipped with RFID tags.[96] The public outcry grew over concerns that the government would use this to track individuals or that passports would get stolen and the data on them copied.[97]

By 2007, RFID had reached its Height of Hysteria and the public's fears about RFID began to diminish. However, privacy fundamentalists, through the media, continued to create micro panics. For example, in 2010, when Wal-Mart finally incorporated RFID into its stores, there was a large spike of activity as the public eye focused once again on the technology. That same year, several local governments also received backlash for trying to use RFID to monitor recycling. For example, Charlotte, North Carolina employed trash tags to "find which areas aren't recycling as often and to start education initiatives there."[98] Many privacy advocates cried foul that this was a veiled attempt to "out" those who failed to properly recycle. According to them, "Bin Brother" was out to get consumers if they mixed up their plastics.

RFID is likely still in its Deflating Fears stage of its privacy panic cycle. People are still getting used to the technology and there are occasional flare-ups of public concern. For example, in 2014 New Hampshire prohibited schools from requiring students to wear identification devices with RFID without going through a public hearing and without the consent of their parents.[99] However, most of these concerns have indeed disappeared. Part of the reason for this is that most concerns never materialized or were proven incorrect. For example, this technology can only be read from a few feet away (as anyone who has unsuccessfully swiped an RFID-enabled transit card or hotel key can confirm). In order to

create a massive tracking system, RFID readers would have to be hidden everywhere. For example, when it came to Levi incorporating the tech into its product supply chain, tags were easily removable and could only be read from within one to three feet.[100] If RFID chips were used as surveillance implants, someone would need to get within a few inches of a reader for the chip to be detected. Therefore, it is impractical to create a surveillance state with this technology.[101] Indeed, there are many reasons why CASPIAN's dystopia never came about.[102]

Most of the negative privacy claims about RFID technology were unsubstantiated, but the benefits afforded by the RFID were very real. Many manufacturers and retailers saw increases in sales and reduced labor costs associated with the roll out of RFID technology. Rather than stopping the rollout of RFID technologies, the industry reacted by creating privacy guidelines for its use.[103] Many retailers started using safeguards, such as "kill codes"—a feature that disarms the RFID's ability to communicate after it leaves the store. Some companies even invented mechanisms to help the industry eliminate privacy risks, such as the global standards organization GS1's Privacy Impact Assessment Tool that helps companies conduct self-assessments of privacy risks associated with RFID technologies.[104] These efforts and benefits, when combined with the fact that fears never materialized, helped to calm the public fears about RFID.

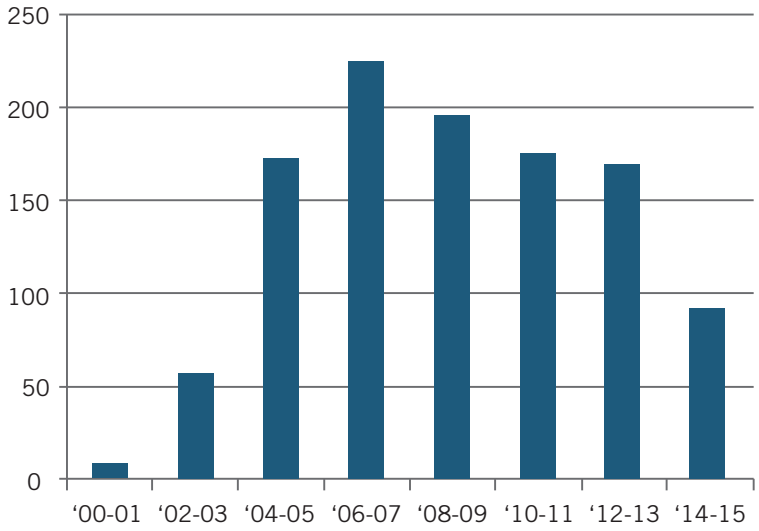

Figure 9: Number of articles on RFID privacy from 2000 to 2015, by two-year period.[105]

The privacy panic cycle is reflected in the news coverage of RFID privacy issues. As shown in figure 9, the number of news articles with the key words "RFID" and "privacy" began climbing around 2003, peaked in 2007, and then has begun to drop off. During this time, RFID deployment faced a series of controversies in which privacy fundamentalists often incorrectly asserted that businesses or government would use RFID chips in an underhanded way to track people's movements, purchases, or habits, and during these times there were occasional spikes in reporting, but there was still a downward trend.

PRIVACY PANIC CYCLES OF CURRENT TECHNOLOGY

Many technologies go through the privacy panic cycle. This section will briefly highlight where 10 technologies reside on the privacy panic cycle.

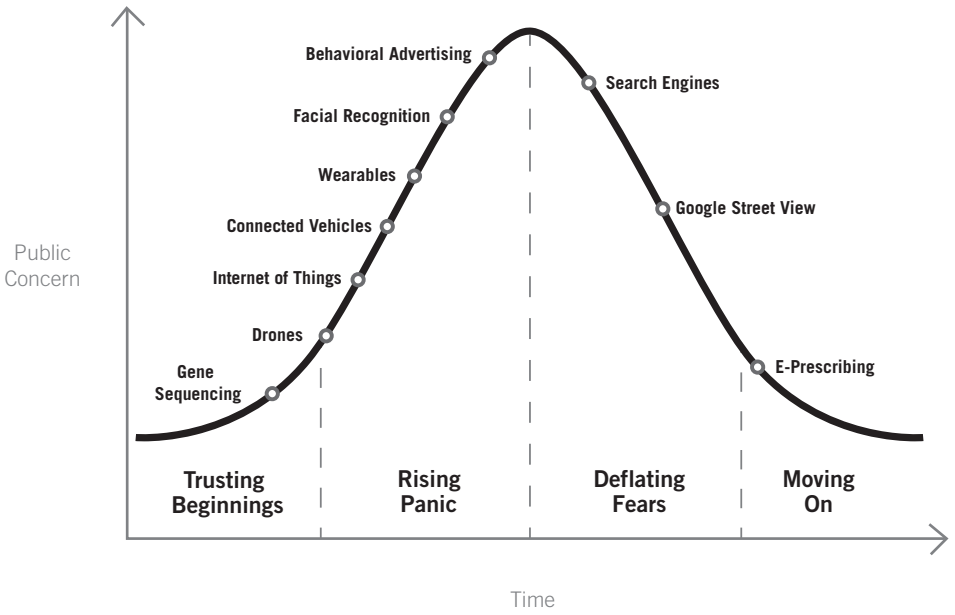

Figure 10: Current technologies on the privacy panic cycle.

Gene Sequencing

Gene sequencing is a relatively nascent technology, and it has only recently become affordable for consumers. In early 2014, the human genome sequencing company Illumina announced it would begin shipping a device capable of sequencing the human genome for under $1,000—a significant drop from a decade earlier when the cost was $10 million.[106] Consumer privacy concerns for this technology are still minimal, as this technology is late in its Trusting Beginnings stage. To be sure, the Presidential Commission for the Study of Bioethical Issues has published extensively on the privacy issues involved with gene sequencing.[107] Several experts and a few media outlets have also published on this issue.[108] But partly because no one has been able to bring this technology to scale and partly because of its obscurity, these concerns have not been elevated to the public consciousness yet. This technology has yet to hit its Point of Panic, at which point these concerns will likely become more widespread.

Drones

Unmanned Aircraft Systems (UAS), commonly referred to as drones, have captured the public's attention, first when Jeff Bezos, the CEO of Amazon, announced in 2013 that he envisioned drones delivering packages to people.[109] Since then, there has been a lively debate about the integration of drones into the U.S. airspace. This debate has been punctuated by a series of events where drones were used in questionable ways, including incidents involving drones flying over the White House grounds and a device laced with

radiation landing on the Japanese Prime Minister's office.[110] Wide-spread commercial drone use is likely still some years away.[111]

However, this has not stopped privacy fundamentalists from raising the alarm over the potential abuse of this technology—by the government or other actors. The American Civil Liberties Union argued, "The prospect of routine aerial surveillance… if unchecked by appropriate legal protections, brings our country a large step closer to a 'surveillance society' in which every move is monitored, tracked, recorded, and scrutinized by the authorities."[112] These fears have started to build outside the realm of privacy fundamentalists, and there has been rapid growth in high-profile press coverage devoted to the privacy concerns associated with drones.[113] Indeed, the Point of Panic with this emerging technology is reflected in President Obama's executive order directing the National Telecommunications and Information Administration (NTIA) to conduct a multistakeholder working group on this technology's privacy issues.[114] The NTIA had conducted one of these meetings at the time of this writing. When the Federal Aviation Administration (FAA), the agency that handles safety issues with all U.S. flights, deferred to the president's order and decided not to include privacy rules as part of its UAS rulemaking, one privacy group sued the FAA asking the regulator to consider privacy rules as part of its rulemaking, instead of only focusing on safety.[115] Furthermore, at least 26 states have passed laws restricting in some way how law enforcement or private citizens can use these devices, often in ways that many drone users call "heavy-handed."[116]

The privacy fears coalescing around drones will continue to build until the technology is integrated into society and commonsense legislation is crafted to mitigate actual harms while protecting innovation.

Given the prevalence of privacy advocates in the debate, the use of privacy rhetoric by policymakers when they discuss the technology, and the frequency of commercial drone coverage by the media, this technology has moved into its Rising Panic stage. Indeed, a 2014 survey found that nearly three-fifths of U.S. adults have privacy concerns about drones, despite only 3 percent of respondents having actually operated one.[117] The privacy fears coalescing around this technology will continue to build until the technology is integrated into society and commonsense legislation is crafted to mitigate actual harms while protecting innovation.

Connected Vehicles

Many car manufacturers have begun to equip their vehicles with Internet connectivity and sensors to allow a host of "infotainment" features such as real-time traffic and weather information, hands-free voice calling, and navigation assistance. These features will not only make travel more comfortable and convenient, they will also improve vehicle safety. For example, a connected vehicle may automatically alert dispatchers in the event of an accident so that first responders can arrive sooner.[118] AT&T has predicted that by 2017, 10 million connected vehicles will be on the roadways.[119] But despite these expected benefits, privacy fundamentalists and some lawmakers have started to raise the alarm over potential privacy issues.

Many privacy fundamentalists have objected to routine collection of data about drivers, especially geolocation information. When California approved Google to operate its autonomous vehicles on the state's highways, one consumer-protection group opposed the approval, saying Google would likely use the opportunity for "collection and use of

voluminous personal information about us and our movements…"[120] Similarly, some privacy fundamentalists worry that vehicle data would be a rich new stream of personal information for governments to generate tickets or prosecute drivers after accidents.[121] In 2015, Sen. Ed Markey (D-MA) released a report saying that the increased connectivity of vehicles is putting the privacy of drivers at risk.[122] As a result, Sen. Markey and Sen. Richard Blumenthal (D-CT) introduced the Security and Privacy in Your Car Act of 2015, (SPY Car Act), to direct federal officials to create IT security and privacy standards for all vehicle electronics and in-vehicle networks.[123]

Based upon how the media, policymakers, and privacy fundamentalists are reacting to this technology, connected vehicles are in the Rising Panic stage.

Internet of Things

The Internet of Things refers to an interconnected environment where all manner of objects are embedded with sensors and transmitters that enable a digital presence and the ability to communicate with other objects and people.[124] The potential for this trend is huge: the number of "things" connected to the Internet is expected to rise to 50 billion by 2020, and to include a vast number of devices from connected cars to intelligent light bulbs and smart trash cans.[125] But since 2009, when the number of connected devices surpassed the number of people, a growing number of privacy fundamentalists have begun talking about this technology. The Internet of Things is in the Rising Panic stage, where the public has begun to express privacy concerns about the Internet of Things without fully understanding its benefits.

People began to refer to Google Glass wearers as "glassholes," a phrase that harkens back to the "Kodak fiends" of the late 1800s.

This stage, as previously discussed, is punctuated by privacy advocates crying wolf, hyperbolic media stories, and policymakers perpetuating needless alarm.[126] This has led the Federal Trade Commission (FTC) to issue a report focusing more on the privacy risks than on the benefits of connected devices.[127] As the technology continues to weave its way into society, people will likely become less concerned about the privacy implications and more comfortable with the technology.

Wearables

Wearables are one subset of the Internet of Things that has advanced past other connected systems in terms of public awareness, privacy concerns, and integration into society. Wearables are on the rise: the number of shipments of wearable devices is expected to grow to 138 million in 2018.[128] Wearable networked devices have surged into the public eye with such notable devices as Apple Watch, Fitbit, Jawbone, and Google Glass. These devices are expected to benefit consumers. For example, one clinician devised a program that offered the Pebble+ fitness tracker to employees who met activity goals, which resulted in reduced medication costs, emergency room visits, and sick days.[129] Similarly, Apple Watch sends warning messages to its wearers when they have been sitting too long, reducing the risk of cancer and high blood pressure associated with prolonged sitting.[130] Google Glass offers opportunities for health care and education, such as live streaming routine surgery for medical students to actively learn.[131]

Privacy fundamentalists have argued that these technologies create serious privacy concerns. For example, I Am The Cavalry (IATC)—a cybersecurity research nonprofit focused on reducing risks related to the Internet of Things—has raised concerns about how these devices are used. Josh Corman, the co-founder of IATC said, "I think what will happen is that there is going to be enough people spied upon by ex-girlfriends or boyfriends, or distrust their government, or get hurt from IoT devices, and we're gonna realize we did too much."[132] Privacy advocates are also concerned that in the rush for cheaper, faster, and smaller devices, companies will not consider the privacy implications of the technology.[133] Adam Tomvim, the CEO of TrustLayers Inc., a Massachusetts-based security company said, "[2015] is going to be the year of privacy by disaster. Instead of everything being designed properly, it's going to be the year where we see quantified-self data leak, and that's when the data-gathering companies are going to realize they need to care for the misuse of the data they collect at the same scale that they analyze the data."[134] These privacy concerns, buoyed along by media coverage devoted to the privacy concerns of wearables have raised the issue into the public consciousness. Indeed, PricewaterhouseCoopers, a multinational professional services network, found in a 2014 survey that 82 percent of U.S. adults were concerned that wearable technologies would invade their privacy.[135] As this evidence shows, wearables are in the Rising Panic stage.

One wearable technology elicited greater privacy panic than most: Google Glass. Many people mistakenly believed that Google Glass constantly records video (which is not feasible with today's batteries).[136] Privacy groups formed to combat this technology. One group, called Stop the Cyborgs, offered free anti-Google Glass signs and art on its website for businesses to notify customers the technology is prohibited.[137] Several states examined whether or not to ban Google Glass behind the wheel or limit the locations in which these devices could be worn or used.[138] Soon several restaurants and bars started to ban them.[139] One such restaurant, the Lost Lake Café & Lounge in Seattle, banned the use of Google Glass while inside, yet encouraged patrons to post photos taken at the business from their smartphones to Instagram and tag them *#LostLake*.[140] People even began to refer to wearers of this technology as "glassholes," a phrase that harkens back to the "Kodak fiends" of the late 1800s.[141] However, over the last decade, wearables have been increasingly accepted into society as people interact positively with them.

Facial Recognition

Facial recognition is a subset of image recognition computer-based technology that is able to automatically detect and identify human faces. This technology, first developed in the 1960s, presents a difficult challenge for computer scientists, because while humans are very good at identifying faces, teaching a computer to do the same is much more difficult.[142] To their credit, since 1960 computer scientists have gotten much better at using technology to recognize similar faces with algorithms. However, throughout it all, privacy fundamentalists have continued to oppose this technical advancement, regardless of the benefits it brings, such as increased security or modest productivity gains on social networks.[143]

Facial recognition technology hit its Point of Panic during the 2001 National Football League's Super Bowl XXXV. The FBI used cameras to take photos of 100,000 fans as they

entered the turnstiles of the event, matching them to known criminals in law enforcement databases and alerting the FBI if there was a match.[144] This event—dubbed the "snooper bowl" by privacy fundamentalists—succeeded in elevating this technology to the national consciousness. In recent years, privacy fundamentalists, helped by the media, have also been concerned with the use of this technology by private companies. For example, Facebook faced their ire when it incorporated this technology into its service to help streamline the photo tagging experience—in which users "tag" or identify their friends in the pictures they post to their profile.[145]

Indeed, policymakers have also delved into this technology. The FTC conducted a workshop and subsequently issued a list of best practices for companies that use facial recognition, including designing their products with security in mind and considering the sensitivity of information when they collect it (e.g., not setting up cameras in places where children play).[146] Similarly, NTIA has organized a stakeholder working group to develop a voluntary code of conduct around the use of facial recognition in many commercial contexts.[147] For example, NTIA set a voluntary code for facial recognition in mobile apps in 2013.[148] In 2015, several consumer privacy groups abandoned the working group because they felt the proposed code of conduct would not do enough to protect privacy.[149]

Facial recognition systems are still in their Rising Panic stage where the media, policymakers, and privacy fundamentalists continue to foment concerns. As the businesses and consumers adopt the technology, people see the convenience offered by this technology, and as it is used to improve security, concerns over its abuse will decrease.

Online Advertising

Online advertising is the predominant funding mechanism of the digital economy, allowing users to enjoy an unlimited amount of free content and services. In order to place the best possible advertisements for individual users and therefore increase their ad revenue and improve their services, websites often track their users' behavior and advertise based on that behavior. However, privacy fundamentalists have consistently railed against the practice, proclaiming that people are both losing their privacy and being hurt by free services that require personal data to properly function.

Privacy fundamentalists argue that companies are guilty of harm simply by gathering personal data, ignoring the facts that these users opt-in to these services and that this information is often used for innocuous purposes. As Marc Rotenberg of the Electronic Privacy Information Center has said, "Businesses will often treat such information as assets. Companies won't say it directly in their privacy policies, but they want people to concede that when you give the company your information, the company owns it and can do what it wants with it."[150] To stop this technology, in 2007, a coalition of consumer privacy groups proposed "Do Not Track"—a single mechanism to opt-out of all online profiling for targeted advertising.[151]

Responding to the concerns, the FTC released a proposed set of rules for industry self-regulation, and the online advertising industry created its own set of principles. By 2010, the Digital Advertising Alliance, a group that represents the online advertising industry,

had codified these rules into an enforceable code of conduct for the industry.[152] With this agreement, the FTC can hold online advertisers responsible for their stated advertising practices and sanction infringing companies.

Despite this, privacy fundamentalists and the media continue to agonize over the information that companies collect on customers. Indeed, government watchdogs from Spain, Italy, France, and Germany, have recently begun investigating the way in which Facebook collects data on its users to deliver relevant advertisements.[153] Behavioral advertising is in its late Rising Panic stage.

Search Engines

Search engines use automated software to index websites, harvesting information as they go. When a user makes a query, the search engine delivers a list of websites ranked in order of relevance to the keywords used in the search. Search engines, such as Google and Bing, make finding information easy and convenient, and allow users to harness the potential of the Internet. However, privacy activists are worried that search engines make consumer information too accessible, while others are uneasy with how long these search engines retain individual search histories. Fears about the records kept by search engines have been around for a long time. The Point of Panic happened when Google introduced a personal search tracker in 2005 that keeps a history of each user's search.[154] In 2006, the Department of Justice asked Google to turn over a week's worth of searches, further sparking outcry from privacy advocates.[155] Privacy fundamentalists and regulators soon began to focus on how long search engines retained their data on individual search histories. In 2007, under pressure brought by European privacy officials and the Federal Trade Commission (the latter of which was spurred to act by complaints from privacy groups), search engines changed the length of time they retained that data.[156] Google changed its policy to anonymize search data that it collects after 18-24 months.[157] Microsoft and AOL also implemented measures to obfuscate user identifying information from search results after 13 to 18 months.[158] Despite these efforts, some privacy groups continued to push for federal legislation to reduce the time companies held this data.[159] In 2008, under pressure to reduce this period from European regulators, Yahoo reduced it to 90 days.[160]

Privacy fundamentalists have raised concerns over the permanence of search listings. Whether due to a youthful mistake or embarrassing photographs, some people want to edit their online past.[161] In May 2014, the European Court of Justice ruled that Europeans have the "right to be forgotten," e.g., the ability to protect their online privacy by requesting search engines to remove links from queries associated with their names if those results are irrelevant, inappropriate, or outdated.[162] Google has since complied with the order on its European domains, reviewing over a quarter of a million removal requests and honored roughly 41 percent of them as of May 2015.[163] Recently, France's privacy regulator called for Google to expand these results to be wiped from every domain worldwide.[164] Privacy advocates have raised these concerns in the United States. In July 2015, Consumer Watchdog, a privacy advocacy organization, sent a letter to the FTC demanding that the government force Google to extend the right to be forgotten to U.S. citizens.[165]

While concerns over search engines have bubbled to the surface recently in Europe, search engines are well understood and frequently used by the majority of Americans. Therefore, because much of the panic cycle has already passed, these fears are less likely to spread. Indeed, as FTC Chairwoman Edith Ramirez has indicated, the right to be forgotten is unlikely to "pass constitutional muster" in the United States due to First Amendment issues.[166] Search engines are likely in their Deflating Fears stage.

Google Street View

Google started gathering imagery for its Google Maps service back in 2007 to allow users to explore Google's online maps as high-resolution panoramic pictures, allowing people to take street-level tours of specific locations from the comfort of their own home.[167] The project, dubbed Street View, initially launched in several cities throughout the United States, but has since expanded to both cities and rural areas globally. Before launching the service, Google put in place easily accessible mechanisms for users to flag inappropriate or sensitive imagery for Google to review and remove.[168] However, the project immediately elicited privacy concerns when it depicted several unedited photographs of people going about their lives: a man picking his nose, protestors outside of an abortion clinic, a couple sunbathing, and men leaving a strip club.[169] Privacy fundamentalists reacted to Google's new service, saying the company had gone too far. For example, in response to Street View, an analyst with the EFF said, "Everyone expects a certain level of anonymity as they move about their daily lives."[170] To be sure, these images were taken on public property and are no different than if a person had captured them on a personal camera while walking down the street.

In 2008, in an attempt to balance user privacy with the online ability to navigate the world, Google introduced a face-blurring technology that obfuscates the identities of people captured in Street View.[171] In addition, Google responded to concerns by blurring license plate numbers, removing personally identifiable details, and even lowering the height of its cameras to avoid capturing photos of people in compromising situations through the windows of their home. Nevertheless, Google continued to face privacy pushback as it rolled out this service worldwide. For example, when Google brought Street View to Europe in 2010, several countries asked the company to purge its unblurred photographs from its databases and post its image-capturing schedule online.[172]

While many concerns over Google's use of real-world imagery have subsided since 2010, some concerns remain.[173] Google's Street View mapping technology is currently in its Deflating Fears stage.

E-Prescribing

Until recently, most doctors would write prescriptions on paper to be delivered by hand or fax, or call them in to a pharmacy. Electronic prescribing (e-prescribing) allows doctors to send a prescription to a pharmacy electronically, thereby improving prescription legibility, boosting efficiency, increasing convenience, and reducing prescription errors.[174] The Institute of Medicine has estimated that 1.5 million preventable adverse drug events—those that result from medical errors—occur in the United States each year and more than 7,000 of those deaths are linked to poor handwriting and prescription filling errors.[175] A

2010 study found that e-prescribing significantly reduced prescription errors, from 37 errors per 100 prescriptions among non-adopters to 7 errors per 100 prescriptions among those who used an e-prescribing system.[176] Furthermore, by sending the prescription directly to pharmacies, e-prescribing improves the rate at which patients take their medicine as prescribed, a costly problem which in the United States contributes to nearly 125,000 deaths per year and $177 billion annually in the form of increased hospitalizations and other complications.[177]

E-prescribing increased following the Medicare Modernization Act, which created standards for e-prescribing that went into effect on January 1, 2006, and established e-prescribing pilot projects.[178] By 2008, health care providers sent approximately 78 million e-prescriptions, more than double the 2007 total of 35 million.[179] Despite the medical community's support for e-prescribing, privacy fundamentalists began opposing these efforts. The Coalition for Patient Privacy, a network of organizations created by the privacy advocacy group Patient Privacy Rights, mounted an opposition movement to vocally denounce e-prescribing as a flagrant attack on patient privacy.[180] For example, Deborah Peel, founder of Patient Privacy Rights, argued fervently that consumers should rally against e-prescriptions because it would allow employers to find out sensitive information about their employees, such as that "they take an anti-anxiety medication or that they are being treated for an STD."[181] She further said, "Would you sit there and watch a house burn down, or let somebody bleed to death before your eyes and do nothing? Or would try to stop those harms? Now that we know beyond a shadow of a doubt that the systemic theft and misuse of personal data is occurring, why wouldn't we do all we can to stop it now, starting with e-prescribing?"[182] Similarly, Tim Sparapani, the former senior legislative counsel for the ACLU, said standardizing patient records into an electronic format would make it easier for pharmacies to sell and trade electronic records, potentially violating patient privacy rights.[183]

These concerns did not stop the rollout of e-prescribing. In 2008, Congress overrode a presidential veto to enact a new Medicare law that, in addition to changing the coverage program, encouraged doctors to write e-prescriptions by increasing payments to physicians using e-prescriptions for their patients.[184] Then, in 2010, the U.S. Drug Enforcement Administration cleared another hurdle by legalizing the e-prescribing of controlled substances.[185] Eventually every state changed its prescribing regulations to develop e-prescription systems that complied with these rules. In 2015, Vermont became the last state to change its rules allowing for the e-prescription of controlled substances.[186]

Privacy concerns over e-prescriptions have declined in recent years, and this technology is currently in the Moving On stage.

CONCLUSION

Newer and better technologies have continued to evolve, but often more slowly than they should because of the objections of privacy fundamentalists and the actions policymakers take on their behalf. Recognizing the privacy panic cycle helps put these fears into perspective. Overblown fears about technology often cloud the judgement of those seeking to understand it, use it, or regulate it. If policymakers do not understand the privacy

panic cycle they are more likely to advocate for policies that have a deleterious effect on innovation.

To be sure, privacy will always continue to be an important consideration as technologies continue to be developed and utilized by both the public and private sector. Concerns for loss of privacy are as valid today as they were with the introduction of the Kodak camera in the late 1800s. However, as policymakers, members of the media, and the population approach new technologies, they should do so with a healthy skepticism of the anticipated downsides and risks the technology will bring. As history has shown, many of the over-inflated claims about loss of privacy have never materialized. Policymakers should not get caught up in the panics that follow in the wake of new technologies, and they should not allow hypothetical, speculative, or unverified claims to color the policies they put in place. Similarly, they should not allow unsubstantiated claims put forth by privacy fundamentalists to derail legitimate public sector efforts to use technology to improve society.

There are a number of reasons that these privacy concerns are rarely realized. First, technologies are often not as powerful as the hype around them suggests. For example, RFID technologies were not used to orchestrate a surveillance society for many reasons, not least because their limited range would make this dystopia infeasible. Second, social norms dissuade many practices that are feasible but undesirable. In addition, businesses are unlikely to surreptitiously gather or use the personal information about their customers in invasive ways if doing so would alienate their consumers and hurt their business. In fact, privacy organizations can do the most good by watching out for real abuses, as opposed to perceived ones, so that organizations know that if they abuse the public's trust, this will likely be widely known. Despite the amount of overblown rhetoric associated with a technology, both public and private institutions have a duty to create commonsense rules that allow the technology to flourish while protecting the public from potential abuse. This means that if applications of these technologies become problematic, regulators and lawmakers will step in to curtail this abuse.

As policymakers and regulators alike look at solving the complex privacy issues brought by emerging technology, they should approach all privacy issues with caution. It is difficult, after all, if not impossible, to predict the pace of technology innovation and how it will affect society. When they do act to limit technology, policymakers should enact narrowly targeted laws and regulations that prevent the privacy abuse of new technologies. This is why—from the Kodak camera to the Internet—most of the most beneficial technologies in history have come from times when entrepreneurs had the freedom to experiment. Heightened fears can often encourage policymakers to propose stifling regulations and to shrink from proactively advancing technological innovation, particularly in sectors with heavy government involvement, such as energy or transportation. As this report has documented, the privacy concerns that emerge from most technological innovations are fleeting at best, and policymakers should consider this as they craft rules and policies in response.

ENDNOTES

1. "72 percent say no to Google Glass because of privacy," *CNET*, April 8, 2014, http://www.cnet.com/news/72-percent-say-no-to-google-glass-because-of-privacy/.
2. For example, activists have delayed the adoption of smart meters that measure energy usage in Nevada. See "Power struggle: Customers vs. NV Energy smart meters," *Fox 5 Las Vegas*, February 6, 2-15, http://www.fox5vegas.com/story/16689913/a-charged-debate-customers-vs-nv-energy-smart-meters.
3. Adam Thierer, "Techno-Panic Cycles (and How the Latest Privacy Scare Fits In)," *the Technology Liberation Front*, February 24, 2011, http://techliberation.com/2011/02/24/techno-panic-cycles-and-how-the-latest-privacy-scare-fits-in/.
4. Scholars have offered several explanations for this phenomenon, including whether a new technology comes along and startles privacy advocates more than the previous technology, the medias' myopic focus on these fears tires out the public, the possibility that our minds can only handle so much fear-mongering, or a combination of all of those factors, but whatever the cause, the fuss eventually subsides and the privacy police move on to the next technology. See Adam Thierer, "Techno-Panic Cycles (and How the Latest Privacy Scare Fits In)," *the Technology Liberation Front.*
5. Tom Standage, "The Culture War," *Wired*, April 2006, http://archive.wired.com/wired/archive/14.04/war.html.
6. "The President's First Sunday in Washington," *New York Times*, September 23, 1901, http://query.nytimes.com/mem/archivefree/pdf?res=9B0CE4DE1E39E733A25750C2A96F9C946097D6CF.
7. Alan Westin, "Social and Political Dimensions of Privacy," *Journal of Social Issues*, Vol. 59, No.2, 2003, http://www.privacysummersymposium.com/reading/westin.pdf.
8. Brad Templeton, "The Evils of Cloud Computing," *BIL Conference*, 2009, video available at https://vimeo.com/3946928.
9. Katherine Albrecht and Liz McIntyre, *Spychips: How major corporations and government plan to track your every move with RFID* (Nashville, TN: Nelson Current, 2005).
10. Thierer, "Technopanics, Threat Inflation, and the Danger of an Information Technology Precautionary Principle," *Mercatus Center*.
11. "Stalkers, Inc." *The Economist*, September 13, 2014, http://www.economist.com/news/leaders/21616953-surveillance-advertising-industrys-new-business-model-privacy-needs-better; Mark Martin, "RFID Opening Doors For Mark of the Beast?" *CBN News*, April 4, 2014, http://www.cbn.com/cbnnews/healthscience/2014/April/RFID-Tech-Opening-Doors-for-Revelation-Fulfillment/, Tim Black, "Are we heading for 'a privacy Chernobyl'?" *Spiked*, March 15, 2010, http://www.spiked-online.com/newsite/article/8310#.VSwhUPnF-Sg.
12. Pictures taken from a variety of media, see Nicolas Loubet, "Big Browser," *Flickr*, October 4, 2011, https://flic.kr/p/asFNQN; "Mark of the Beast! Hidden RFID Chip Tracking, Exposed in Obamacare!" *Youtube*, https://www.youtube.com/watch?v=UYFOje2_zTw; Josh Bell, "Domestic Drones: Hear About Who's Watching You from Above," *American Civil Liberties Union*, December 21, 2011, https://www.aclu.org/blog/domestic-drones-hear-about-whos-watching-you-above; "No Surveillance Devices," *Stop the Cyborgs*, accessed July 21, 2015, https://stopthecyborgs.files.wordpress.com/2013/05/surveillance-ban.png.
13. "From how far away can a typical RFID tag be read?" *RFID Journal*, accessed August 3, 2015, http://www.rfidjournal.com/faq/show?139.
14. Will Oremus, "Was a Texas Student Really Expelled for Refusing To Wear an RFID Chip?" *Slate*, November 30, 2012, http://www.slate.com/blogs/future_tense/2012/11/30/rfid_in_texas_schools_was_andrea_hernandez_expelled_for_refusing_to_wear.html.
15. Donna Wentworth, "Gmail: What's the Deal?" *Electronic Frontier Foundation*, April 5, 2004, https://www.eff.org/deeplinks/2004/04/gmail-whats-deal.
16. Beth Givens, "Thirty-One Privacy and Civil Liberties Organizations Urge Google to Suspend Gmail," *Privacy Rights Clearinghouse*, April 6, 2004, https://www.privacyrights.org/ar/GmailLetter.htm.
17. Julian Hattem, "With half of House, Lawmakers push email privacy bill," *The Hill*, February 04, 2015, http://thehill.com/policy/technology/231677-with-half-of-house-lawmakers-push-email-privacy-bill.
18. Jane Hadley, "'Loyalty cards cause griping over swiping," *Seattle Pi*, May 10, 2002, http://www.seattlepi.com/news/article/Loyalty-cards-cause-griping-over-swiping-1087086.php;

"Frequently Asked Questions About CASPIAN," *Spychips*, accessed August 3, 2015, http://www.spychips.com/about_us.html.

19. Bruno Giussanli, "Camera Phones Raise Privacy Concerns," *Wall Street Journal*, July 28, 2003, http://www.wsj.com/articles/SB105934395032309500.
20. Unfamiliarity and apprehension can prevent adoption of a technology amongst a population until they realize the technologies benefits. See, David Douglas and Karen Paullet, "RFID Ubiquity and Privacy Loss Concerns: An Analysis of a Pennsylvania University," *Issues in Information Systems*, Volume XI, No. 1, 2010, 113-117, http://iacis.org/iis/2010/111-118_LV2010_1419.pdf.
21. Christopher Maag, "Surprise! Your GPS Device (Probably) Isn't Spying On You," *Business Insider*, June 3, 2011, http://www.businessinsider.com/surprise-your-gps-device-probably-isnt-spying-on-you-2011-6.
22. Chris Hayes, "Before PRISM there was Total Information Awareness," *MSNBC*, September 2, 2013, http://www.msnbc.com/all-in/prism-there-was-total-information-awar.
23. Staff Writers, "Google Rolls Out New Privacy Policy Amid Howls," *Consumer Watchdog*, March 1, 2012, http://www.consumerwatchdog.org/story/google-rolls-out-new-privacy-policy-amid-howls; "Google Copies Your Hard Drive - Government Smiles in Anticipation" *Electronic Frontier Foundation*, February 9, 2006, https://www.eff.org/press/archives/2006/02/09; David Coursey, "Privacy: Why Google Social Search Gives me the Creeps," *PC World*, October 27, 2009, http://www.pcworld.com/article/174476/Privacy_Why_Google_Social_Search_Gives_Me_The_Creeps.html; Seeing Through Windows, "Chrome: Google's biggest threat to your privacy," *Computerworld*, September 4, 2008, http://www.computerworld.com/article/2480353/internet/chrome--google-s-biggest-threat-to-your-privacy.html.
24. Tracy Miller, "Improving the Efficiency and Equity of Highway Funding and management," *Mercatus Center*, February 2014, http://mercatus.org/sites/default/files/Miller_VMT_v1.pdf.
25. Anthony Ferraro, "Electronic Commerce: The Issues and Challenges to Creating Trust and A Positive Image in Consumer Sales on the World Wide Web," *First Monday*, June 1, 1998, http://firstmonday.org/ojs/index.php/fm/article/view/601/522.
26. David Brooks, "The Lost Language of Privacy," *New York Times*, April 14, 2015, http://www.nytimes.com/2015/04/14/opinion/david-brooks-the-lost-language-of-privacy.html?ref=opinion.
27. Justin Sink, "Obama to provide funding for 50,000 police body cameras," *The Hill*, December 1, 2014, http://thehill.com/homenews/administration/225583-obama-to-provide-funding-for-50000-police-body-cameras; Jon Fingas, "Hillary Clinton wants all police to wear body cameras," *Engadget*, April 29, 2015, http://www.engadget.com/2015/04/29/hillary-clinton-wants-police-body-cameras/.
28. Matt Winkeljohn, "Obamacare Mandatory RFID Chipping Now Being Implemented In Wyoming," *Before its News*, July 28, 2013, http://beforeitsnews.com/science-and-technology/2013/07/obamacare-mandatory-rfid-chipping-now-being-implemented-in-wyoming-2622262.html.
29. Zachary Stieber, "Are RFID Chips Being Tested for Obamacare? No, It's a Hoax," *Epoch Times*, November 7, 2013, http://www.theepochtimes.com/n3/350269-are-rfid-chips-being-tested-for-obamacare-no-its-a-hoax/.
30. "RFID Chip Now Being Issued In Hanna, Wyoming As Part Of New "Obamacare" Plan," *National Report*, July 2013, http://nationalreport.net/rfid-chip-now-being-issued-in-hanna-wyoming-as-part-of-new-obamacare-plan/#sthash.h84rxakA.dpuf
31. "Is Big Brother in your grocery cart?" *CASPIAN*, accessed May 28, 2015, http://www.nocards.org/; Robert Atkinson, "The 2014 ITIF Luddite Awards," *Information Technology and Innovation Foundation*, January 2015, http://www2.itif.org/2015-luddite-awards.pdf?_ga=1.107889410.1240521073.1404749065.
32. "With speed-of-light technological innovation, information privacy is becoming more complex by the minute as more data is being collected and exchanged. As the technology gets more sophisticated (indeed, invasive), so do the uses of data. And that leaves organizations facing an incredibly complex risk matrix for ensuring that personal information is protected." See, "About the IAPP," *International Association of Privacy Professionals*, accessed May 28, 2015, https://privacyassociation.org/about/what-is-privacy.
33. "Baltimore Start-Up Aims To Put Users in Control of Online Tracking," *IAPP Blog*, July 22, 2015, https://iapp.org/news/a/baltimore-startup-aims-to-give-users-control-to-stop-online-tracking/. And see, for example, Ghostplate at http://www.ghostplate.com/, accessed August 24, 2015.

34. Julia Angwin and Emily Steel, "Web's Hot New Commodity: Privacy," *Wall Street Journal*, February 28, 2011, http://www.wsj.com/articles/SB10001424052748703529004576160764037920274.
35. The *Wall Street Journal* offered a series of articles on digital privacy including "What They Know," "the End of Privacy," and "Watched." See, "What They Know," *Wall Street Journal*, accessed July 10, 2015, http://www.wsj.com/public/page/what-they-know-digital-privacy.html.
36. For example, the Wall Street Journal's "What They Know" investigation rated its own websites "exposure index" as a "medium"—the same as Yahoo, MSN, Amazon, and MySpace. See "What They Know" table at http://blogs.wsj.com/wtk/ accessed August 24, 2015.
37. Farhad Manjoo, "Everything is Watching YOU," *Salon*, July 24, 2003, http://www.salon.com/2003/07/24/rfid/.
38. "Another person, who formerly served on the board of an oft-quoted privacy watchdog, related that privacy alarms were part of the group's fund-raising strategy." Jeff John Roberts, "Why privacy settlements like Facebook's "Sponsored Stories" lawsuit aren't working," *GigaOM*, September 19, 2013, https://gigaom.com/2013/09/19/why-privacy-settlements-like-facebooks-sponsored-stories-lawsuit-arent-working/.
39. Ibid.
40. Lori Andrews, "Privacy and Technology: A 125-Year Review," *CK Privacy*, 2013, http://www.ckprivacy.org/uploads/4/1/8/3/41830523/andrews_then__now_final.pdf; Guided by the privacy concerns from the onset of the portable camera, two legal scholars—Louis Brandeis and Samuel Warren, both of whom later sat on the Supreme Court—wrote a law journal article called "The Right to Privacy." This article argued that new technology had created privacy harm, and that "instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life." Warren and Brandeis's work would set the precedent for how governments, businesses, and advocates approach privacy law across the country to this day. See, Louis Brandeis and Samuel Warren, "The Right to Privacy," *Harvard Law Review*, Vol. 4 No. 5, December 15, 1890, http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html
41. David Lindsay, "The Kodak Camera Starts a Craze," *Public Broadcasting Service*, accessed May 28, 2015, http://www.pbs.org/wgbh/amex/eastman/peopleevents/pande13.html.
42. Clive Thompson, "The Invention of the "Snapshot" Changed the Way We Viewed the World," *Smithsonian*, September 2014, http://www.smithsonianmag.com/innovation/invention-snapshot-changed-way-we-viewed-world-180952435/?all.
43. Ibid.
44. Clive Thompson, "The Invention of the "Snapshot" Changed the Way We Viewed the World," *Smithsonian.*
45. Ibid.
46. Picture taken from "Patents: George Eastman and the Roll Film Camera," *GENi*, September 4, 2014, http://www.geni.com/blog/patents-george-eastman-and-the-roll-film-camera-385961.html.
47. Elizabeth Brayer, *George Eastman: A Biography* (New York: University of Rochester Press, 2006), 70.
48. Ibid, 72.
49. "'Kodak Fiends' At Newport," *New York Times*, August 18, 1899, http://query.nytimes.com/mem/archivefree/pdf?res=9507E0D61F3DE433A2575BC1A96E9C94689ED7CF.
50. "Have you seen the Kodak fiend!" *Hawaiian Gazette*, December 6, 1890, http://chroniclingamerica.loc.gov/lccn/sn83025121/1890-12-09/ed-1/seq-5/.
51. Nick Bilton, "Disruptions: At Odds Over Privacy Challenges of Wearable Computing," *New York Times*, May 26, 2013, http://bits.blogs.nytimes.com/2013/05/26/disruptions-at-odds-over-privacy-challenges-of-wearable-computing/
52. David Lindsay, "The Kodak Camera Starts a Craze," *Public Broadcasting Service.*
53. Clive Thompson, "The Invention of the "Snapshot" Changed the Way We Viewed the World," *Smithsonian.*
54. David Lindsay, "The Kodak Camera Starts a Craze," *Public Broadcasting Service*.
55. Clive Thompson, "The Invention of the "Snapshot" Changed the Way We Viewed the World," *Smithsonian;* John Updike, "Visual Trophies," *New Yorker*, December 24, 2007, http://www.newyorker.com/magazine/2007/12/24/visual-trophies.

56. Clive Thompson, "The Invention of the "Snapshot" Changed the Way We Viewed the World," *Smithsonian.*
57. David Lindsay, "The Kodak Camera Starts a Craze," *Public Broadcasting Service.*
58. For example, one person wrote in the journal *Photography* in 1938, long after the initial privacy hoopla, "Candid photography is making us human goldfish." John Updike, "Visual Trophies," *New Yorker.*
59. Alan Westin, "Social and Political Dimensions of Privacy," *Journal of Social Issues*, Vol. 59, No. 2, 2003, 1-30, http://www.privacysummersymposium.com/reading/westin.pdf.
60. Ibid, 164-165.
61. John Neary, "The Big Snoop: Electronic Snooping – Insidious Invasions of Privacy," *Life Magazine*, May 20, 1966, http://www.bugsweeps.com/info/life_article.html.
62. Smith, 164-165.
63. Neary, "The Big Snoop: Electronic Snooping – Insidious Invasions of Privacy," *Life Magazine*.
64. Ibid.
65. Ibid.
66. Ibid.
67. Lyndon Baynes Johnson, "State of the Union Address," *Public Broadcasting Service*, 1967, accessed May 28, 2015, http://www.pbs.org/wgbh/americanexperience/features/primary-resources/lbj-union67/.
68. "Long Calls Missouri Defeat 'Victory for Snooper'," *New York Times*, August 8, 1968, http://timesmachine.nytimes.com/timesmachine/1968/08/08/76960417.html?pageNumber=26.
69. Smith, 178-179.
70. Ibid.
71. Ibid, 165.
72. Cathy Booth-Thomas, "The See-It-All Chip," *TIME*, September 14, 2003, http://content.time.com/time/magazine/article/0,9171,485764-1,00.html.
73. Ibid.
74. Bob Violino, "The History of RFID Technology," *RFID Journal*, January 16, 2005, http://www.rfidjournal.com/articles/view?1338.
75. Booth-Thomas, "The See-It-All Chip," *TIME.*
76. Ibid.
77. Bob Violino, "Using RFID Tags to Prevent Theft," *RFID Journal*, July 12, 2003, https://www.rfidjournal.com/purchase-access?type=Article&id=499&r=%2Farticles%2Fview%3F499.
78. The Rutherford Institute, a nonprofit civil liberties organization, summarized this idea: an individual's acceptance of a certain code—a unique identifier—as a pass conferring certain privileges from a secular ruling authority was some "form of idolatry or submission to a false god." See "Andrea Hernandez Stands Firm, Asks School Officials to Respect Her Religious Objections to RFID Tracking Program, Let Her Use Old Badge & Stay in School," *The Rutherford Institute*, January 18, 2013, https://www.rutherford.org/files_images/general/11-21-2012_TRO-Petition_Hernandez.pdf.
79. Booth-Thomas, "The See-It-All Chip," *TIME*.
80. Katherine Albrecht and Liz McIntyre, *Spychips: How major corporations and government plan to track your every move with RFID* (Nashville, TN: Nelson Current, 2005).
81. Mark Martin, "RFID Opening Doors for Mark of the Beast?" *CBN News*, April 4, 2014, http://www.cbn.com/cbnnews/healthscience/2014/April/RFID-Tech-Opening-Doors-for-Revelation-Fulfillment/.
82. Katherine Albrecht, *I Won't Take the Mark: A Bible Book and Contract for Children* (Virtue Press, 2014); Albrecht and McIntyre, *Spychips: How major corporations and government plan to track your every move with RFID.*
83. Miguel Bustillo, "Wal-Mart Radio Tags to Track Clothing," *Wall Street Journal*, July 23, 2010, http://www.wsj.com/articles/SB10001424052748704421304575383213061198090; Farhad Manjoo, "Everything is watching YOU," *Salon*, July 24, 2003, http://www.salon.com/2003/07/24/rfid/; Cathy Booth-Thomas, "The See-It-All Chip," *TIME;* Barnaby Feder," A Debate We Don't Need: Do RFID Chips in Humans Cause Cancer," *New York Times*, September 10, 2007, http://bits.blogs.nytimes.com/2007/09/10/a-debate-we-dont-need-do-rfid-chips-in-humans-cause-cancer/?; Parija Bhatnagar, "Spies on a store shelf?", *CNN Money*, September 23, 2004, http://money.cnn.com/2004/09/07/news/fortune500/retail_rfid/; Jonathan Krim, "Embedding Their

Hopes In RFID," *Washington Post*, June 23, 2004, http://www.washingtonpost.com/wp-dyn/articles/A62061-2004Jun22_3.html; Katherine Albrecht, "How RFID Tags Could Be Used to Track Unsuspecting People," *Scientific American*, September 2008, http://www.scientificamerican.com/article/how-rfid-tags-could-be-used/.

84. Jane Black, "Playing Tag with Shoppers' Anonymity," *Bloomberg Business*, July 20, 2003, http://www.bloomberg.com/bw/stories/2003-07-20/playing-tag-with-shoppers-anonymity.
85. Black, "Playing Tag with Shoppers' Anonymity," *Bloomberg Business*; and Miguel Bustillo, "Wal-Mart Radio Tags to Track Clothing," *Wall Street Journal*, July 23, 2010, http://www.wsj.com/articles/SB10001424052748704421304575383213061198090.
86. "RFID and consumers: understanding their mindset. A U.S. Study examining consumer awareness and perceptions of radio frequency identification technology," *CapGemini Ernst & Young*, 2004, http://www.slideshare.net/PeterSam67/rfid-and-consumers-understanding-their-mindset.
87. Ibid.
88. "CASPIAN Announced Worldwide Tesco Boycott on BBC Television," *Boycott Tesco*, January 26, 2005, http://www.boycotttesco.com/press-release.html.
89. Andrew Donoghue, "Privacy activists demand Tesco boycott over RFID," *ZDNet*, January 26, 2005, http://www.zdnet.com/article/privacy-activists-demand-tesco-boycott-over-rfid/;
90. Laurie Sullivan, "Levi Ships RFID-Tagged Jeans," *Information Week*, April 28, 2006, http://www.informationweek.com/levi-ships-rfid-tagged-jeans/d/d-id/1042704.
91. Albrecht, "How RFID Tags Could Be Used to Track Unsuspecting People," *Scientific American*.
92. Beth Bacheldor, "Wisconsin Bill to Ban Coerced Chip Implants," *RFID Journal*, May 2, 2006, http://www.rfidjournal.com/articles/view?2304; Orr Shtuhl, "California could become third state to ban forced microchip tag implants," *Global Research*, January 12, 2008, http://www.globalresearch.ca/california-could-become-third-state-to-ban-forced-microchip-tag-implants-rfid/7781; David Chartier, "Washington State passes RFID privacy law; where's Uncle Sam?" *Arstechnica*, March 28, 2008, http://arstechnica.com/security/2008/03/washington-state-passes-rfid-privacy-law-wheres-uncle-sam/.
93. Lorna Martin, "This chip makes sure you always buy your round," *The Guardian*, January 15, 2005, http://www.theguardian.com/science/2005/jan/16/theobserver.theobserversuknewspages.
94. Jeffrey Kahn, "Implanting ideas to store medical history," *CNN*, May 13, 2002, http://edition.cnn.com/2002/HEALTH/05/13/ethics.matters/.
95. Jo Best, "Civil liberties groups unite for RFID protest," *ZDNet*, March 31, 2004, http://www.zdnet.com/article/civil-liberties-groups-unite-for-rfid-protest/.
96. Jon Stokes, "US offers RFID passports to the public," *Arstechnica*, August 14, 2006, http://arstechnica.com/uncategorized/2006/08/7497/.
97. Ibid.
98. John Brandon, "Cities Increasingly Turn to 'Trash Police' to Enforce Recycling Laws," *Fox News*, September 8, 2010, http://www.foxnews.com/tech/2010/09/07/trash-police-invade-thanks-government-stimulus/.
99. New Hampshire Rev, Stat. 189:68, http://www.gencourt.state.nh.us/rsa/html/XV/189/189-68.htm.
100. Charlie White, "Levi's Testing Clothing with RFID Tags," *Gizmodo*, May 04, 2006, http://gizmodo.com/171574/levis-testing-clothing-with-rfid-tags
101. In 2006, the Wall Street Journal reported that one man feared that his credit card—which was embedded with a radio chip—would accidentally pay for someone else's gas if he walked by or thieves would use it to pay for the gas at his expense. Despite the fact that cards would have to get within inches of the pump for this to be realized, this fear led many to purchase wallets with metal shields to block radio signals. Many others took a hammer to their chips, at the direction of CASPIAN, to disable the radio frequency. See, Susan Warren, "Why Some People Put These Credit Cards In the Microwave," *Wall Street Journal*, April 10, 2006, http://www.wsj.com/articles/SB114463085998921417.
102. Rob Atkinson, "RFID: There's Nothing to Fear Except Fear Itself," *Information Technology and Innovation Foundation*, May 4, 2006, http://www.itif.org/files/rfid.pdf.
103. "Tagged Item Performance Protocol," *The Global Language of Business*, March 12, 2014, http://www.gs1us.org/industries/apparel-general-merchandise/workgroups/item-level-rfid/tagged-item-performance-protocol.

104. Claire Swedberg, "GS1 Releases Privacy-Assessment Tool for RFID Users," *RFID Journal*, November 23, 2011, http://www.rfidjournal.com/articles/view?8986.
105. This graph was the result of an ITIF survey of Google search results featuring the terms "privacy" and "RFID" between 2000 and 2014. The researcher removed false-positive results that were a product of website "privacy" statements.
106. Liat Clark, "Illumina announces landmark $1,000 human genome sequencing," *Wired*, January 15, 2014, http://www.wired.co.uk/news/archive/2014-01/15/1000-dollar-genome; and "NHGRI Seeks Next Generation of Sequencing Technologies," *National Human Genome Research Institute*, October 14, 2004, http://www.genome.gov/12513210.
107. "Privacy and Progress in Whole Genome Sequencing," *Presidential Commission for the Study of Bioethical Issues*, October 2012, http://bioethics.gov/sites/default/files/PrivacyProgress508_1.pdf.
108. Amy Gutmann and James Wagner, "Found Your DNA on the Web: Reconciling Privacy and Progress," *The Hastings Center*, no. 3, 2013, 15-18, http://www.thehastingscenter.org/Publications/HCR/Detail.aspx?id=6343&terms=Gutmann+and+%23filename+*.html; Sharon Begley, "Citing privacy concerns, U.S. panel urges end to secret DNA testing," *Reuters*, October 22, 2012, http://www.reuters.com/article/2012/10/11/us-usa-geneticprivacy-idUSBRE89A06H20121011.
109. David Pierce, "Delivery drones are coming: Jeff Bezos promises half-hour shipping with Amazon Prime Air," *The Verge*, December 1, 2013, http://www.theverge.com/2013/12/1/5164340/delivery-drones-are-coming-jeff-bezos-previews-half-hour-shipping
110. Kristen Holmes, "Man detained outside White House for trying to fly drone," *CNN*, May 15, 2015, http://www.cnn.com/2015/05/14/politics/white-house-drone-arrest/; Dustin Volz, "A Drone Is the Latest White House Fence-Jumper," *National Journal*, January 26, 2015, http://www.nationaljournal.com/tech/a-drone-is-the-latest-white-house-fence-jumper-20150126; "Drone laced with radiation lands on Japan PM's office," *Aljazeera*, April 22, 2015, http://www.aljazeera.com/news/2015/04/drone-laced-radiation-lands-japan-pm-office-150422185726666.html.
111. The Government Accountability Office predicts that we cannot expect to completely integrate commercial drones into America's skies until 2017 or later. See, Gerald Dillingham, "Efforts Made toward Integration into the National Airspace Continue, but Many Actions Still Required," *U.S. Government Accountability Office*, December 10, 2014, http://gao.gov/assets/670/667346.pdf.
112. Christopher R. Calabrese, "The Future of Unmanned Aviation in the U.S. Economy: Safety and Privacy Considerations," *American Civil Liberties Union*, January 15, 2014, https://www.aclu.org/sites/default/files/assets/domestic_drones_statement_senate_commerce_committee.pdf.
113. "A Looming Threat," *The Economist*, November 22, 2015, http://www.economist.com/blogs/democracyinamerica/2015/03/drones-and-privacy.
114. "Presidential Memorandum: Promoting Economic Competitiveness While Safeguarding Privacy, Civil Rights, and Civil Liberties in Domestic Use of Unmanned Aircraft Systems," *The White House*, February 15, 2015, https://www.whitehouse.gov/the-press-office/2015/02/15/presidential-memorandum-promoting-economic-competitiveness-while-safegua
115. Jack Nicas, "Privacy Group Sues FAA Over Drone Rules," *Wall Street Journal*, March 31, 2015, http://www.wsj.com/articles/privacy-group-sues-faa-over-drone-rules-1427845718; "Electronic Privacy Information Center v. the Federal Aviation Administration," *U.S. Court of Appeals for the District of Columbia Circuit*, March 31, 2015, https://epic.org/privacy/litigation/apa/faa/drones/EPIC-v-FAA-DC-Cir-Petition.PDF.
116. Jack Nicas, "Drones Boom Raises New Question: Who Owns Your Airspace?", *Wall Street Journal*, May 13, 2015, http://www.wsj.com/articles/drones-boom-raises-new-question-who-owns-your-airspace-1431535417; "Current Unmanned Aircraft State Law Landscape," *National Conference of State Legislatures*, August 26, 2015, http://www.ncsl.org/research/transportation/current-unmanned-aircraft-state-law-landscape.aspx.
117. Joan Lowy and Jennifer Agiesta, "AP-GFK Poll: Americans skeptical of commercial drones," *Associated Press*, December 19, 2014, http://ap-gfkpoll.com/featured/findings-from-our-latest-poll-10.

118. Craig Timberg, "Web-connected cars bring privacy concerns," *Washington Post*, March 5, 2013, http://www.washingtonpost.com/business/technology/web-connected-cars-bring-privacy-concerns/2013/03/05/d935d990-80ea-11e2-a350-49866afab584_story.html.
119. Juan Martinez, "AT&T: 'Expect 10 million connected cars by 2017'," *Tech Radar*, September 10, 2014, http://www.techradar.com/news/car-tech/at-t-expect-10-million-connected-cars-by-2017--1261833.
120. Jamie Court and John Simpson, "SB 1298; oppose unless amended," *Consumer Watchdog*, May 30, 2012, http://www.consumerwatchdog.org/resources/ltrgoogdrive053012.pdf.
121. Craig Timberg, "Web-connected cars bring privacy concerns," *Washington Post.*
122. Ed Markey, "Tracking and Hacking: Security and Privacy Gaps Put American Drivers at Risk," *U.S. Senate*, February 2015, http://www.markey.senate.gov/imo/media/doc/2015-02-06_MarkeyReport-Tracking_Hacking_CarSecurity%202.pdf.
123. S. 1806, 114th Congress (2015), http://www.markey.senate.gov/imo/media/doc/SPY%20Car%20legislation.pdf.
124. Daniel Castro and Jordan Misra, "Internet of Things," *Center for Data Innovation*, November 2013, http://www2.datainnovation.org/2013-internet-of-things.pdf.
125. Dave Evans, "The Internet of Things: How the Next Evolution of the Internet is Changing Everything," *Cisco*, April 2011, http://www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf.
126. Corynne McSherry, "Who Will Own the Internet of Things? (Hint: Not the Users)," *Electronic Frontier Foundation*, January 20, 2015, https://www.eff.org/deeplinks/2015/01/who-will-own-internet-things-hint-not-users; Danny Bradbury, "How can privacy survive in the era of the internet of things," *The Guardian*, April 7, 2015, http://www.theguardian.com/technology/2015/apr/07/how-can-privacy-survive-the-internet-of-things; Lauren Zanolli, "Welcome to Privacy Hell, Also Known as the Internet of Things," *Fast Company*, March 23, 2015, http://www.fastcompany.com/3044046/tech-forecast/welcome-to-privacy-hell-otherwise-known-as-the-internet-of-things; Grant Gross, "Senators to push privacy, security legislation for IoT, connected cars," *PC World*, February 11, 2015, http://www.pcworld.com/article/2883352/senators-to-push-privacy-security-legislation-for-iot.html.
127. Daniel Castro, "Statement in Response to FTC's Internet of Things Staff Report," *Center for Data Innovation*, press release, January 27, 2015, http://www.datainnovation.org/2015/01/statement-in-response-to-ftcs-internet-of-things-staff-report/.
128. Hugo Deacon, "Smartwatches and Smart Bands Dominate Fast-Growing Wearables Market," *CCS Insight*, August 2014, http://www.ccsinsight.com/press/company-news/1944-smartwatches-and-smart-bands-dominate-fast-growing-wearables-market.
129. Marley Jay, "Fitness trackers are hot, but do they really help?" *WNYT TV*, June 18, 2015, http://wnyt.com/article/stories/s3829776.shtml.
130. Mike Darling, "The Apple Watch Lives Up to the Hype," *Men's Health*, April 24, 2015, http://www.menshealth.com/techlust/apple-watch-review.
131. Erica Gavin, "5 Medical Specialties That Can Benefit from Google Glass," *HIT Consultant*, June 30, 2015, http://hitconsultant.net/2014/06/03/5-medical-specialties-that-can-benefit-from-google-glass/.
132. Lauren Zanolli, "Welcome to Privacy Hell, Also Known as the Internet of Things," *Fast Company*, March 23, 2015, http://www.fastcompany.com/3044046/tech-forecast/welcome-to-privacy-hell-otherwise-known-as-the-internet-of-things.
133. Ibid.
134. Amber Hunt, "Experts: Wearable tech tests our privacy limits," *USA Today*, February 5, 2015, http://www.usatoday.com/story/tech/2015/02/05/tech-wearables-privacy/22955707/.
135. "The Wearable Future," *PricewaterhouseCoopers*, 2014, http://www.pwc.com/en_US/us/technology/publications/assets/pwc-wearable-tech-design-oct-8th.pdf.
136. Heather Kelly, "Google Glass users fight privacy fears," *CNN*, December 12, 2013, http://www.cnn.com/2013/12/10/tech/mobile/negative-google-glass-reactions/.
137. "Google Glass ban signs," *Stop The Cyborgs*, accessed May 19, 2015, http://stopthecyborgs.org/google-glass-ban-signs/.
138. Jacob Gershman, "Proposed Google Glass Driving Bans Are 'Unenforceable,' Says Professor," *Wall Street Journal*, August 13, 2014, http://blogs.wsj.com/law/2014/08/13/proposed-google-glass-driving-restrictions-are-unenforceable-says-professor/.

139. Richard Gray, "The places where Google Glass is banned," *The Telegraph*, December 4, 2013, http://www.telegraph.co.uk/technology/google/10494231/The-places-where-Google-Glass-is-banned.html.
140. Kelly, "Google Glass users fight privacy fears," *CNN*.
141. Whitney Boesel, "Google Glass Doesn't Have a Privacy Problem. You Do," *TIME*, May 19, 2014, http://time.com/103510/google-glass-privacy-foregrounding/.
142. "Face Recognition," *Federal Bureau of Investigations*, accessed July 9, 2015, https://www.fbi.gov/about-us/cjis/fingerprints_biometrics/biometric-center-of-excellence/files/face-recognition.pdf.
143. Daniel Castro, "No Longer A Nameless Face In the Crowd," *Innovation Files*, June 11, 2011, http://www.innovationfiles.org/no-longer-a-nameless-face-in-the-crowd/.
144. Vickie Chachere, "Biometrics Used to Detect Criminals at Super Bowl," *ABC News*, February 13, 2001, http://abcnews.go.com/Technology/story?id=98871.
145. Sarah Jacobsson Purewal, "Why Facebook's Facial Recognition is Creepy," *PC World*, June 8, 2011, http://www.pcworld.com/article/229742/Why_Facebooks_Facial_Recognition_is_Creepy.html.
146. Federal Trade Commission, "FTC Recommends Best Practices for Companies That Use Facial Recognition Technologies," news release, October 22, 2012, https://www.ftc.gov/news-events/press-releases/2012/10/ftc-recommends-best-practices-companies-use-facial-recognition.
147. "Privacy Multistakeholder Process: Facial Recognition Technology," *National Telecommunications & Information Administration*, June 11, 2015, http://www.ntia.doc.gov/other-publication/2015/privacy-multistakeholder-process-facial-recognition-technology.
148. "Short Form Notice Code of Conduct to Promote Transparency in Mobile App Practices," *National Telecommunications & Information Administration*, July 25, 2015, http://www.ntia.doc.gov/files/ntia/publications/july_25_code_draft.pdf.
149. Elizabeth Weise, "Privacy groups leave over dispute on facial recognition software," *USA Today*, June 16, 2015, http://www.usatoday.com/story/tech/2015/06/16/facial-recognition-software-google-facebook-moments-ntia/28793157/.
150. David Lazarus, "It's time to take ownership of our personal data," *Los Angeles Times*, April 6, 2012, http://articles.latimes.com/2012/apr/06/business/la-fi-lazarus-20120406.
151. Daniel Castro, "'Do-Not-Track' Legislation: Is Now The Right Time?" *The Information Technology and Innovation Foundation*, December 2, 2010, http://www.itif.org/files/2010-do-not-track-testimony.pdf.
152. "Digital Advertising Alliance Begins Enforcing Next Phase of Self-Regulatory Program for Online Behavioral Advertising," *Digital Advertising Alliance*, May 23, 2011, http://www.aboutads.info/resource/download/DAA_Compliance_FINAL.pdf.
153. Arjun Kharpal, "Europe privacy probes could 'derail' Facebook revenue growth," *CNBC*, June 23, 2015, http://www.cnbc.com/2015/06/23/europe-privacy-probes-could-derail-facebook-revenue-growth.html.
154. Antone Gonsalves, "Google Personal-Search Tracker Raises Privacy Concerns," *Information Week*, April 21, 20005, http://www.informationweek.com/google-personal-search-tracker-raises-privacy-concerns/d/d-id/1032093.
155. Adam Liptak, "In Case About Google's Secrets, Yours Are Safe," *New York Times*, January 26, 2006, http://www.nytimes.com/2006/01/26/technology/26privacy.html.
156. Ryan Singel, "Search Engine Privacy Changes Driven by Competition, Lawmakers & Lawsuits, Advocacy Group Reports," *Wired*, August 8, 2007, http://www.wired.com/2007/08/search-engine-p.
157. Peter Fleischer and Nicole Wong, "Taking Steps to Further Improve our Privacy Practices," *Google*, March 14, 2007, http://googleblog.blogspot.com/2007/03/taking-steps-to-further-improve-our.html.
158. Ryan Singel, "Search Engine Privacy Changes Driven by Competition, Lawmakers & Lawsuits, Advocacy Group Reports," *Wired*.
159. Ari Schwartz and Alissa Cooper, "Search Privacy Practices: A Work in Progress," *Center for Democracy and Technology*, August 2007, https://www.cdt.org/files/privacy/20070808searchprivacy.pdf.
160. Miguel Helft, "Yahoo Limits Retention of Search Data," *New York Times*, December 17, 2008, http://www.nytimes.com/2008/12/18/technology/internet/18yahoo.html.
161. Jeffrey Toobin, "The Solace of Oblivion," *New Yorker*, September 29, 2014, http://www.newyorker.com/magazine/2014/09/29/solace-oblivion.

162. Alan Travis and Charles Arthur, "EU court backs 'right to be forgotten': Google must amend results on request," *The Guardian*, May 13, 2014, http://www.theguardian.com/technology/2014/may/13/right-to-be-forgotten-eu-court-google-search-results.
163. Levi Sumagaysay, "Google 'right to be forgotten' removals: 41 percent in the past year," *Siliconbeat*, May 13, 2015, http://www.siliconbeat.com/2015/05/13/google-right-to-be-forgotten-removals-41-percent-in-the-past-year/.
164. Alan McQuinn, "France should not force its internet policies on the world," *Europolitics*, June 25, 2015, http://europolitics.info/france-should-not-force-its-internet-policies-world.
165. John Simpson, "Complaint Regarding Google's Failure To Offer 'Right To Be Forgotten' In The U.S," *Consumer Watchdog,* July 7, 2015, http://www.consumerwatchdog.org/resources/ltrftcrtbf070715.pdf.
166. Victor Luckerson, "Meet the Woman Keeping Silicon Valley in Check," *Time*, July 26, 2014, http://time.com/3040669/ftc-edith-ramirez/.
167. Stephen Chau, "Introducing… Street View!" *Google*, May 29, 2007, http://google-latlong.blogspot.com/2007/05/introducing-street-view.html.
168. Elinor Mills, "Google's street-level maps raising privacy concerns," *USA Today*, June 4, 2007, http://usatoday30.usatoday.com/tech/news/internetprivacy/2007-06-01-google-maps-privacy_N.htm.
169. Michael Liedtke, "Google hits streets, raises privacy concerns," *NBC News*, June 1, 2007, http://www.nbcnews.com/id/18987058/ns/technology_and_science-security/t/google-hits-streets-raises-privacy-concerns/#.Va0olflVhBc.
170. Ibid.
171. Stephen Shankland, "Google begins blurring faces in Street View," *CNET*, May 13, 2008, http://www.cnet.com/news/google-begins-blurring-faces-in-street-view/.
172. Tony Bradley, "Google Street View Raises Privacy Concerns… Again," *PCWorld*, February 26, 2010, http://www.pcworld.com/article/190279/Google_Street_View_Raises_Privacy_ConcernsAgain.html.
173. Google also settled a dispute brought by 38 states over its data gathering practices related to personal information that the company gathered over WiFi using cars outfitted with cameras for Street View. See, David Streitfeld, "Google Concedes That Drive-By Prying Violated Privacy," *New York Times*, March 12, 2013, http://www.nytimes.com/2013/03/13/technology/google-pays-fine-over-street-view-privacy-breach.html.
174. "What are some of the benefits of e-prescribing?" *U.S. Department of Health and Human Services*, accessed September 1, 2015, http://www.hrsa.gov/healthit/toolbox/HealthITAdoptiontoolbox/ElectronicPrescribing/benefitsepres.html.
175. "Preventing Medication Errors," *Institute of Medicine*, July 2006, http://iom.nationalacademies.org/~/media/Files/Report%20Files/2006/Preventing-Medication-Errors-Quality-Chasm-Series/medicationerrorsnew.pdf; Amber Porterfield, Kate Engelbert, and Alberto Coustasse, "Electronic Prescribing: Improving the Efficiency and Accuracy of Prescribing in the Ambulatory Care Setting," *Perspectives in Health Information Management*, April 1, 2014, http://www.ncbi.nlm.nih.gov/pmc/articles/PMC3995494/#B31.
176. Rainu Kaushal et al., "Electronic Prescribing Improves Medication Safety in Community-Based Office Practices," *Journal of General Internal Medicine*, Volume 26 (6), June 2010, http://www.ncbi.nlm.nih.gov/pmc/articles/PMC2869410/?tool=pubmed.
177. Regina Benjamin, "Medication Adherence: Helping Patients Take Their Medicines As Directed ," *Public Health Reports*, Volume 127(1), January 2012, http://www.ncbi.nlm.nih.gov/pmc/articles/PMC3234383/#B2; "Enhancing Prescription Medicine Adherence: A Narional Action Plan," *National Council on Patient Information and Education*, August 2007, http://www.talkaboutrx.org/documents/enhancing_prescription_medicine_adherence.pdf; Surescripts, "Study: E-Prescribing Shown to Improve Outcomes and Save Healthcare System Billions of Dollars," news release, February 1, 2012, http://surescripts.com/news-center/press-releases/!content/212_eprescribing.
178. "E-Prescribing," *Centers for Medicare & Medicaid Services*, February 26, 2014, https://www.cms.gov/Medicare/E-health/Eprescribing/index.html.
179. "What are some of the benefits of e-prescribing?" *U.S. Department of Health and Human Services.*

180. "Letters," *Patient Privacy Rights*, accessed August 31, 2015, https://patientprivacyrights.org/letters/; "Letter to Representative Neil Abercrombie," *Coalition for Patient Privacy,* October 18, 2007, http://patientprivacyrights.org/wp-content/uploads/2013/08/Microsoft-Word-Letter-to-Congress-Final-10-17.07.pdf.
181. "2007/2008 Coalition," *Patient Privacy Rights*, accessed August 31, 2015, https://patientprivacyrights.org/2007-2008-coalition/.
182. Patient Privacy Rights, "25 National Organizations Urge Privacy in E-Prescribing," news release, May 13, 2008, http://patientprivacyrights.org/wp-content/uploads/2013/08/e-rx_press_release1.pdf.
183. Janet Kornblum, "Writing is on the wall for doctors' e-prescriptions," *USA Today*, July 29, 2008, http://usatoday30.usatoday.com/news/health/2008-07-28-eprescribe_N.htm.
184. Anne Mathews and Jane Zhang, "How Changes In Medicare Affect Patients," *Wall Street Journal*, July 17, 2008, http://www.wsj.com/articles/SB121623946819959433.
185. "Electronic Prescriptions for Controlled Substances," *U.S. Drug Enforcement Administration*, accessed August 31, 2015, http://www.deadiversion.usdoj.gov/ecomm/e_rx/.
186. Neil Versel, "Vermont becomes final state to legalize e-prescribing of controlled substances," *MedCity News*, August 28, 2015, http://medcitynews.com/2015/08/vermont-e-prescribing-of-controlled-substances/.

ACKNOWLEDGMENTS

The authors wish to thank the following individuals for providing input to this report: Rob Atkinson and Randolph Court. Any errors or omissions are the authors' alone.

ABOUT THE AUTHORS

Daniel Castro is the vice president of the Information Technology and Innovation Foundation. His research interests include health IT, data privacy, e-commerce, e-government, electronic voting, information security, and accessibility. Before joining ITIF, Castro worked as an IT analyst at the Government Accountability Office (GAO) where he audited IT security and management controls at various government agencies. He has a B.S. in Foreign Service from Georgetown University and an M.S. in Information Security Technology and Management from Carnegie Mellon University.

Alan McQuinn is a research assistant with the Information Technology and Innovation Foundation. His research areas include a variety of issues related to emerging technology and Internet policy, such as cybersecurity, privacy, virtual currencies, e-government, and commercial drones. Prior to joining ITIF, McQuinn was a telecommunications fellow for Congresswoman Anna Eshoo and an intern for the Federal Communications Commission in the Office of Legislative Affairs. He got his B.S. in Political Communications and Public Relations from the University of Texas at Austin.

ABOUT ITIF

The Information Technology and Innovation Foundation (ITIF) is a Washington, D.C.-based think tank at the cutting edge of designing innovation strategies and technology policies to create economic opportunities and improve quality of life in the United States and around the world. Founded in 2006, ITIF is a 501(c) 3 nonprofit, non-partisan organization that documents the beneficial role technology plays in our lives and provides pragmatic ideas for improving technology-driven productivity, boosting competitiveness, and meeting today's global challenges through innovation.

FOR MORE INFORMATION, VISIT US AT WWW.ITIF.ORG.