MERCATUS CENTER
George Mason University
Bridging the gap between academic ideas and real-world problems

PUBLIC INTEREST COMMENT

PRIVACY AND SECURITY IMPLICATIONS OF THE INTERNET OF THINGS

By Adam Thierer

Federal Trade Commission
Comment period closes June 1, 2013

INTRODUCTION

The Federal Trade Commission (FTC) has requested comments regarding "the consumer privacy and security issues posed by the growing connectivity of consumer devices, such as cars, appliances, and medical devices," in anticipation of a November 21 public workshop on "the Internet of Things."[1]

The Technology Policy Program of the Mercatus Center at George Mason University is dedicated to advancing knowledge about the effects of regulation on society. As part of its mission, the program conducts careful and independent analyses that employ contemporary economic scholarship to assess agency rulemakings and proposals from the perspective of the public interest. Therefore, this comment on the FTC's "Internet of Things" (IoT) proceeding does not represent the views of any particular affected party or special interest group but is designed to assist the agency as it explores these issues.

While it is unclear what may come from this proceeding, the danger exists that it represents the beginning of a regulatory regime for a new set of information technologies that are still in their infancy. Fearing hypothetical worst-case scenarios about the misuse of some IoT technologies, some policy activists and policymakers could seek to curb or control their development.

To that extent, we write to make the simple point that the Internet of Things—like the Internet itself—should not be subjected to a precautionary principle, which would impose preemptive, prophylactic restrictions on this rapidly evolving sector to guard against every theoretical harm that could develop. Preemptive restrictions on the development of the Internet of Things could retard technological innovation and limit the benefits that flow to consumers. Policymakers should instead exercise restraint and humility in the face of uncertain change and address harms that develop—if they do at all—after careful benefit-cost analysis of various remedies.[2]

[1] Federal Trade Commission, "FTC Seeks Input on Privacy and Security Implications of the Internet of Things," April 17, 2013, http://ftc.gov/opa/2013/04/internetthings.shtm.

[2] Adam Thierer, "A Framework for Benefit-Cost Analysis in Digital Privacy Debates," *George Mason University Law Review* (forthcoming, Summer 2013).

For more information, contact:
Taylor Barkley, (703) 993-8205, tbarkley@mercatus.gmu.edu
Mercatus Center at George Mason University
3351 Fairfax Drive, 4th Floor, Arlington, VA 22201

The ideas presented in this document do not represent official positions of the Mercatus Center or George Mason University.

THE INTERNET OF THINGS: AN EVOLVING CONCEPT

The Internet of Things is an evolving concept. Analysts have noted that “there are almost as many interpretations of the term ‘Internet of Things’ as there are experts and interested parties”[3] and that it has “some fuzziness, and can have different facets depending on the perspective taken.”[4]

Generally speaking, however, the Internet of Things “is a term for when everyday ordinary objects are connected to the Internet” via microchips and sensors[5] and “the point in time when more ‘things or objects’ [are] connected to the Internet than people.”[6] The Internet of Things is sometimes viewed as being synonymous with “smart” systems, such as “smart homes,” “smart buildings,” “smart health,” “smart grids,” “smart mobility,” and so on.[7]

The promise of the Internet of Things, as described by *New York Times* reporter Steve Lohr, is that “billions of digital devices, from smartphones to sensors in homes, cars, and machines of all kinds, will communicate with each other to automate tasks and make life better.”[8] According to Cisco, by 2020, 37 billion intelligent things will be connected and communicating.[9] Thus, we are rapidly approaching the point where “everyone and everything will be connected to the network.”[10]

Examples of the Internet of Things are already visible[11] in the form of remote home monitoring technologies;[12] wearable computing (like Google Glass);[13] self-tracking tools (like Nike+ and Fitbit) and sensor-rich fabric;[14]

[3] BCS–The Chartered Institute for IT & Oxford Internet Institute, *The Societal Impact of the Internet of Things*, February 2013, 2.

[4] RFID Working Group of the European Technology Platform on Smart Systems Integration, *Internet of Things in 2020: A Roadmap for the Future*, September 5, 2008, 6, http://www.smart-systems-integration.org/public/documents/publications/Internet-of-Things_in_2020_EC-EPoSS_Workshop_Report_2008_v3.pdf.

[5] Richard MacManus, "Top 10 Internet of Things Developments of 2010," *ReadWrite.com*, December 15, 2010, http://readwrite.com/2010/12/15/top_10_internet_of_things_developments_of_2010.

[6] Dave Evans, "The Internet of Things: How the Next Evolution of the Internet Is Changing Everything," Cisco White Paper, April 2011, 2, http://www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf.

[7] Ian G. Smith (ed.), The Internet of Things 2012 - *New Horizons* (Internet of Things European Research Cluster, 2012), at 29-31.

[8] Steve Lohr, "A Messenger for the Internet of Things," *New York Times*, April 25, 2013, http://bits.blogs.nytimes.com/2013/04/25/a-messenger-for-the-internet-of-things.

[9] Dave Evans, "Thanks to IoE, the Next Decade Looks Positively ‘Nutty’," *Cisco Blog*, February 12, 2013, http://blogs.cisco.com/ioe/thanks-to-ioe-the-next-decade-looks-positively-nutty.

[10] RFID Working Group, *Internet of Things* in 2020, 21.

[11] See generally Julie Bort, "Everything You Need to Know about the New Internet—The ‘Internet of Things’," *Business Insider*, March 29, 2013, http://www.businessinsider.com/what-you-need-to-know-about-the-internet-of-things-2013-3?op=1; W. David Stephenson, *SmartStuff: An Introduction to the Internet of Things* (June 20, 2012), http://www.amazon.com/SmartStuff-introduction-Internet-Things-ebook/dp/B008DDW2U2.

[12] Sarah Kessler, "Your House: The Next Great Digital Network," *Mashable*, May 24, 2012, http://mashable.com/2012/05/24/smart-objects-startups; Lauren Indvik, "5 Connected Objects to Smarten Up Your Home," *Mashable*, January 20, 2013, http://mashable.com/2013/01/20/smart-home; Stacey Higginbotham, "AT&T Launches Its Internet of Things Effort and It's Pretty Big," *GigaOm*, April 25, 2013, http://gigaom.com/2013/04/25/att-launches-its-internet-of-things-effort-and-its-pretty-big.

[13] Olga Kharif, "Wearable Tech Market May Swell to $6B by 2016," *Washington Post*, May 13, 2012, http://www.washingtonpost.com/business/google-glass-woos-developers-to-6-billion-wearable-market-tech/2013/05/13/e475a7ac-bb84-11e2-b537-ab47f0325f7c_story.html?wpisrc=nl_politics (noting that "the wearable-computer market may swell to $6 billion by 2016, according to Wellingborough, U.K.-based IMS Research," and that "some 70 million connected wearable gadgets will be sold in 2017, up from 15 million this year, according to Juniper Research").

[14] Stacey Higginbotham, "You Call Google Glass Wearable Tech? Heapsylon Makes Sensor-Rich Fabric," *GigaOm*, May 16, 2013, http://gigaom.com/2013/05/16/you-call-google-glass-wearable-tech-heapsylon-makes-sensor-rich-fabric.

intelligent energy[15] and power systems;[16] autonomous vehicles;[17] retail tracking and automated inventory management systems;[18] and much more.[19] Importantly, innovation in this space is already occurring at an extremely rapidly pace, thanks to the same underlying drivers of the Internet economy, namely Moore's Law and Metcalfe's Law.[20]

The benefits that will accrue to society from the growth of the Internet of Things will be enormous.[21] "As people and context-aware machines gain access to more actionable information," says Cisco CEO John Chambers, "the result will be new capabilities, richer experiences, and unprecedented value for individuals, businesses, communities and countries everywhere."[22]

Some of the most exciting developments in this space involve the use of digital sensors to improve health and safety. For example, ABI Research reports that:

> The market for disposable wireless Medical Body Area Network (MBAN) sensors within professional healthcare is in its earliest stages, but key foundations to support adoption are now in place. [. . .] MBAN sensors will enable patient monitoring information such as temperature to be collected automatically from a wearable thermometer sensor. These devices will improve patient monitoring detail and free up nursing staff to concentrate on other aspects of care. By bringing the technology to disposable form factors MBAN sensors integrate especially well with the workflow of professional healthcare.[23]

IDC Government Insights also explains the potential benefits for assisted living for elderly or for patients that are seriously ill. "Wearable readers (known as e-bandages) can measure body temperature, blood pressure, heart

[15] Dahai Han, Jie Zhang, Yongjun Zhang, and Wanyi Gu, "Convergence of Sensor Networks/Internet of Things and Power Grid Information Network at Aggregation Layer," Power System Technology (POWERCON), 2010 International Conference on Power System Technology, October 2010, http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=5666553.

[16] Katie Fehrenbacher, "The Internet of Things and Energy," *GigaOm*, October 10, 2011, http://gigaom.com/2011/10/10/the-internet-of-things-energy.

[17] Thilo Koslowski, "Forget the Internet of Things: Here Comes the 'Internet of Cars'," *Wired*, January 4, 2013, http://www.wired.com/opinion/2013/01/forget-the-internet-of-things-here-comes-the-internet-of-cars; Marshall Kirkpatrick, "Google's Self-Driving Car Is Just the Beginning," *ReadWrite.com*, October 11, 2010, http://readwrite.com/2010/10/11/googles_self-driving_car_where_it_stands_in _histor.

[18] Jeff Bertolucci, "Internet of Things Wake-Up Call For Enterprises," *Information Week*, May 13, 2013, http://www.informationweek.com/big-data/news/big-data-analytics/internet-of-things-wakeup-call-for-enterprises/240154763.

[19] Clive Thompson, "No Longer Vaporware: The Internet of Things Is Finally Talking," *Wired*, December 6, 2012, http://www.wired.com/opinion/2012/12/20-12-st_thompson. ("In essence, the Internet of Things is happening because it has reached the 'Apple II stage.' This is the moment when a new technology finally becomes easy enough to use that thousands of people start doing experiments to scratch a personal itch—like Sande with his fan. And the pace of experimentation is going to accelerate, as new gear arrives that makes it even cheaper and easier.")

[20] Michael Chui, Markus Löffler, and Roger Roberts, "The Internet of Things," *McKinsey Quarterly*, March 2010, http://www.mckinsey.com/insights/high_tech_telecoms_internet/the_internet_of_things. ("The widespread adoption of the Internet of Things will take time, but the time line is advancing thanks to improvements in underlying technologies. Advances in wireless networking technology and the greater standardization of communications protocols make it possible to collect data from these sensors almost anywhere at any time. Ever-smaller silicon chips for this purpose are gaining new capabilities, while costs, following the pattern of Moore's Law, are falling. Massive increases in storage and computing power, some of it available via cloud computing, make number crunching possible at very large scale and at declining cost.") BCS & Oxford Internet Institute, Societal Impact of the Internet of Things, 4. ("New developments around the IoT will move faster than the relevant law and policy, creating a challenge to governance and policy in this area. The regulatory processes that were designed to cope with hundreds or thousands of transactions or services providers might need to be reconsidered in order to cope with a trillion things and the data they produce.")

[21] David Kirkpatrick, "Why an Internet of Everything Event? 'It's the World Waking Up'," *Forbes*, May 9, 2013, http://www.forbes.com/sites/techonomy/2013/05/09/why-an-internet-of-everything-event-its-the-world-waking-up.

[22] John Chambers, "Internet of Everything: Fueling an Amazing Future #TomorrowStartsHere," *Cisco Blog*, December 12, 2012, http://blogs.cisco.com/news/internet-of-everything-2.

[23] ABI Research, "Disposable Wireless Sensor Market Shows Signs of Life – Healthcare Shipments to Reach 5 Million in 2018," May 3, 2013, http://www.abiresearch.com/press/disposable-wireless-sensor-market-shows-signs-of-l.

rhythm and other parameters and be combined with environmental sensor to measure moisture, temperature, movement, sound and GPS embedded in mobile phones to monitor movements inside and outside of the home."[24]

Autonomous vehicles and automated driving systems, which must be constantly connected to networks in order to operate, also promise to help save lives and money.[25] Analysts with the McKinsey Global Institute have noted that imminent collision detection and automatic braking systems in cars "mimic human reactions, though at vastly enhanced performance levels."[26] As a result, "The potential accident reduction savings flowing from wider deployment could surpass $100 billion annually."[27] IoT technologies could also have a variety of environmental benefits by encouraging greater conservation and carbon reduction efforts.[28]

The IoT will also have profound ramifications for governments—especially city and county governments—by making it easier to create "smart cities" and administer public services far more efficiently.[29]

WHICH POLICY DEFAULT: PERMISSIONLESS INNOVATION OR THE PRECAUTIONARY REGULATION?

These are just a few examples of how society will benefit from the growth of the Internet of Things. Of course, as was the case with many other new information and communications technologies, the initial impulse may instead be to curb or control the development of certain IoT systems to guard against theoretical future misuses or harms that might develop.

When such fears take the form of public policy prescriptions, it is referred to as a "precautionary principle."[30] The precautionary principle generally holds that, because a given new technology could pose some theoretical danger or risk in the future, public policies should control or limit the development of such innovations until their creators can prove that they won't cause any harms.

The problem with letting such precautionary thinking guide policy is that it poses a serious threat to technological progress, economic entrepreneurialism, and human prosperity.[31] Under an information policy regime guided at every turn by a precautionary principle, technological innovation would be impossible because of fear of the unknown; hypothetical worst-case scenarios would trump all other considerations.[32] Social learning and economic opportunities become far less likely, perhaps even impossible, under such a regime. In practical terms, it means

[24] "Internet Of Things Reaching Tipping Point: IDC," BIZTECH2.com, Apr. 29, 2013, http://biztech2.in.com/news/enterprise-solutions/internet-of-things-reaching-tipping-point-idc/157622/0.

[25] Timothy B. Lee, "Self-Driving Cars are a Privacy Nightmare. And It's Totally Worth It," *Washington Post*, May 21, 2013, http://www.washingtonpost.com/blogs/wonkblog/wp/2013/05/21/self-driving-cars-are-a-privacy-nightmare-and-its-totally-worth-it (noting that "while that will alarm some privacy advocates, the benefits of self-driving cars dwarf the potential harms. Cars driven by human beings kill about 30,000 people each year. Self-driving technology could dramatically reduce that figure. Self-driving technology will enable expanded car-sharing, saving thousands of acres currently wasted on parking lots. And the technology will free up billions of person-hours currently devoted to the drudgery of commuting every year.").

[26] Chui, Löffler, and Roberts, "The Internet of Things," *McKinsey Quarterly*.

[27] Ibid.

[28] W. David Stephenson, "New Report Projects Major Greenhouse Gas Cuts with M2M Implementation," *stephenson blogs on Internet of Things, data, et al.*, March 19, 2013, http://www.stephensonstrategies.com/new-report-projects-major-greenhouse-gas-cuts-with-m2m-implementation.

[29] Duncan Jefferies, "How the 'Internet of Things' Could Radically Change Local Government," *The Guardian*, August 18, 2011, http://www.guardian.co.uk/local-government-network/2011/aug/18/internet-of-things-local-government; Marjorie Censer, "Companies Pitch Cities on Going High Tech," *Washington Post*, May 19, 2013, http://www.washingtonpost.com/business/on-it/companies-pitch-cities-on-going-high-tech/2013/05/19/62c75c32-b1d4-11e2-bbf2-a6f9e9d79e19_story.html.

[30] Adam Thierer, "Technopanics, Threat Inflation, and the Danger of an Information Technology Precautionary Principle," *Minnesota Journal of Law, Science & Technology* 14, no. 1 (2013).

[31] Jonathan H. Adler, "The Problems with Precaution: A Principle Without Principle," *The American*, May 25, 2011, http://www.american.com/archive/2011/may/the-problems-with-precaution-a-principle-without-principle.

[32] Cass R. Sunstein, *Laws of Fear: Beyond the Precautionary Principle* (2005).

fewer services, lower quality goods, higher prices, diminished economic growth, and a decline in the overall standard of living.[33]

For these reasons, to the maximum extent possible, the default position toward new forms of technological innovation should be *innovation allowed*. This policy norm is better captured in the well-known Internet ideal of "permissionless innovation," or the general freedom to experiment and learn through trial-and-error experimentation.[34]

Stated differently, when it comes to the Internet of Things, the default policy position should be an "*anti*-Precautionary Principle." Paul Ohm, who recently joined the FTC as a Senior Policy Advisor, outlined the concept in his 2008 article, "The Myth of the Superuser: Fear, Risk, and Harm Online."[35] "Fear of the powerful computer user, the 'Superuser,' dominates debates about online conflict," Ohm argued, but this superuser is generally "a mythical figure" concocted by those who are typically quick to set forth worst-case scenarios about the impact of digital technology on society.[36] Fear of such superusers and the hypothetical worst-case dystopian scenarios they might bring about prompts policy action, since "policymakers, fearful of his power, too often overreact by passing overbroad, ambiguous laws intended to ensnare the Superuser but which are instead used against inculpable, ordinary users."[37] "This response is unwarranted," Ohm says, "because the Superuser is often a marginal figure whose power has been greatly exaggerated."[38]

SOCIETAL ADAPTATION

Unfortunately, fear of "superusers" and worst-case boogeyman scenarios are already driving much of the debate over the Internet of Things.[39] Yet patience and openness to permissionless innovation still represent the wise disposition here, not only because it provides breathing space for future entrepreneurialism, but also because it provides an opportunity to observe both the evolution of societal attitudes toward this new technology and how citizens adapt to it. It is likely that citizen attitudes about these emerging technologies will follow a familiar cycle we have seen play out in other contexts of initial *resistance*, gradual *adaptation*, and then eventual *assimilation* of that new technology into society.[40]

In the extreme, the initial resistance to new technologies takes the form of a "technopanic," which refers to "an intense public, political, and academic response to the emergence or use of media or technologies, especially by the young."[41] Many of these panics have been premised on safety, security, or privacy concerns. Or, more simply, new technologies were sometimes initially resisted because they disrupted long-standing social norms.

Despite the worst-case scenarios and hypothetical fears, individuals adapted in almost every case and assimilated new technologies into their lives. This is true even for new devices and services that initially raised very serious

[33] Adam Thierer, "Who Really Believes in 'Permissionless Innovation'?" *Technology Liberation Front*, March 4, 2013, http://techliberation.com/2013/03/04/who-really-believes-in-permissionless-innovation.

[34] Eli Dourado, "'Permissionless Innovation' Offline as Well as On," *The Umlaut*, February 6, 2013. ("Advocates of the Internet are right to extol the permissionless innovation model—but they are wrong to believe that it need be unique to the Internet. We can legalize innovation in the physical world, too. All it takes is a recognition that real-world innovators should not have to ask permission either.")

[35] Paul Ohm, "The Myth of the Superuser: Fear, Risk, and Harm Online," *University of California-Davis Law Review* 41 (2008): 1327–402.

[36] Ibid, 1327.

[37] Ibid.

[38] Ibid, 1327.

[39] See generally Bruce Schneier, "Will Giving the Internet Eyes and Ears Mean the End of Privacy?" *The Guardian*, May 16, 2013, http://www.guardian.co.uk/technology/2013/may/16/internet-of-things-privacy-google; Mike Wheatley, "Big Brother's Big Data: Why We Must Fear the Internet of Things," *Silicon Angle*, January 10, 2013, http://siliconangle.com/blog/2013/01/10/big-brothers-big-data-why-we-must-fear-the-internet-of-things.

[40] Adam Thierer, "Technopanics, Threat Inflation, and the Danger of an Information Technology Precautionary Principle," *Minnesota Journal of Law, Science & Technology* 14, no. 1 (2013): 309–86.

[41] Thierer, "Technopanics," 311.

privacy concerns. As technology author Larry Downes has observed, "After the initial panic, we almost always embrace the service that once violated our visceral sense of privacy."[42]

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

- **The telephone:** While many modern media and communications technologies have challenged well-established norms and conventions, few were as socially disruptive as the telephone. Writing recently in *Slate*, Keith Collins has noted that, "when the telephone was invented, people found the concept entirely bizarre. So much so that the first telephone book, published in 1878, had to provide instructions on how to begin and end calls. People were to say 'Ahoy' to answer the phone and 'That is all' before hanging up."[43] But people quickly adjusted to the new device. "Ultimately, the telephone proved too useful to abandon for the sake of social discomfort," notes Collins. "It was also something people could to get used to in their own homes. They didn't have to overcome the awkwardness in public . . . That was a barrier another device would have to deal with 100 years later."[44] Of course, when cell phones did come along 100 years later, people got over that "awkwardness," too.

- **Cameras / public photography:** The introduction and evolution of the camera and photography provides another useful example of social adaptation. The camera was initially viewed as a highly disruptive force when photography became more widespread in the late 1800s. Indeed, the most important essay ever written on privacy law, Samuel D. Warren and Louis D. Brandeis's famous 1890 *Harvard Law Review* essay on "The Right to Privacy," decried the spread of the device.[45] The authors lamented that "instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life" and claimed that "numerous mechanical devices threaten to make good the prediction that 'what is whispered in the closet shall be proclaimed from the house-tops.'"[46] But personal norms and cultural attitudes toward cameras and public photography evolved quite rapidly and they became an ingrained part of the human experience. At the same time, social norms and etiquette evolved to address those who would use cameras in inappropriate, privacy-invasive ways.

- **Caller ID:** Although caller identification tools are widely used today, they were the subject of a heated privacy debate in the 1990s.[47] The Electronic Privacy Information Center and other privacy advocates wanted the Federal Communications Commission to block the revelation of telephone numbers by default and to opt-in to allow their phone numbers be displayed.[48] Today, caller ID is a routine feature in not just traditional phones but all phone apps for smartphones.[49]

- **RFID:** When radio-frequency identification (RFID) technologies first came on the scene in the early 2000s, a brief panic followed. In the extreme, RFID was likened to the biblical threat of the "mark of the beast."[50] Legislative bills to regulate privacy-related aspects of RFID technology were introduced in several states, although none passed.[51] Fears about RFID were greatly exaggerated and the panic largely

[42] Larry Downes, "A Rational Response to the Privacy 'Crisis,'" Cato Institute *Policy Analysis* No. 716, January 7, 2013, 10.

[43] Keith Collins, "OK, Glass, Don't Make Me Look Stupid," *Slate*, May 14, 2013, http://www.slate.com/articles/technology/future_tense/2013/05/google_glass_social_norms_will_it_be_too_awkward_to_use_in_public.html.

[44] Ibid.

[45] Samuel D. Warren & Louis D. Brandeis, "The Right to Privacy," *Harvard Law Review* 4 (1890): 193.

[46] Ibid, 195.

[47] S. J. Diamond, "What's Behind the Fuss Over Caller ID," *Los Angeles Times*, June 15, 1990, http://articles.latimes.com/1990-06-15/business/fi-370_1_caller-id-units; Matthew L. Wald, "Caller ID Reaches Out a Bit Too Far," *New York Times*, February 2, 1995, http://www.nytimes.com/1995/02/02/nyregion/caller-id-reaches-out-a-bit-too-far.html.

[48] Electronic Privacy Information Center, "Called ID," http://epic.org/privacy/caller_id (last accessed May 17, 2013).

[49] Jane Yakowitz Bambauer, "Is Data Speech?" *Stanford Law Review* 66 (forthcoming, 2013): 59.

[50] Mark Baard, "RFID: Sign of the (End) Times?" *Wired*, June 6, 2006, http://www.wired.com/science/discoveries/news/2006/06/70308.

[51] Declan McCullagh, "Don't Regulate RFID—Yet," *CNET News*, April 30, 2004, http://news.cnet.com/Don%27t%20regulate%20RFID--yet/2010-1039_3-5327719.html.

passed within a few years.[52] Today, RFID technologies represent the foundation upon which many other IoT systems and technologies are being developed.[53]

- **Gmail:** When Google launched its Gmail service in 2004, it was greeted with hostility by many privacy advocates and some policymakers.[54] Rather than charging some users for more storage or special features, Google paid for the service by showing advertisements next to each email "contextually" targeted to keywords in that email. Some privacy advocates worried that Google was going to "read users' email," however, and pushed for restrictions on such algorithmic contextual targeting.[55] But users enthusiastically embraced Gmail and the service grew rapidly. By the summer of 2012, Google announced that 425 million people were actively using Gmail.[56] Users adapted their privacy expectations to accommodate this new service, which offered them clear benefits (free service, generous storage, and improved search functionality) in exchange for tolerating some targeted advertising.

- **Wireless location-based services:** In Spring 2011, Apple and Google came under fire for retaining location data gleaned by iPhone- and Android-based smartphone devices.[57] But these "tracking" concerns were greatly overblown since almost all mobile devices must retain a certain amount of locational information to ensure various services work properly, and this data was not being shared with others.[58] Of course, those users who are highly sensitive about locational privacy can always turn off locational tracking or encrypt and constantly delete their data.[59] But most consumers now routinely use wireless location-based services, regardless of privacy concerns.

These case studies prove that, more often than not, society has found ways to adapt to new technological changes by employing a variety of coping mechanisms or new social norms. These examples should give us hope that we will also find ways of adapting to the challenges presented by the rise of the Internet of Things.

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

HOW NORMS "REGULATE"

Importantly, new technologies can be regulated by more than just law. As suggested above, social pressure and private norms of acceptable use often act as "regulators" of the uses (and misuses) of new technologies. This was clearly the case for the camera. Even as they became widely used and accepted through social adaptation, it is also the case that certain uses of cameras were socially discouraged or curtailed by private norms.

[52] See generally Jerry Brito, "Relax, Don't Do It: Why RFID Privacy Concerns are Exaggerated and Legislation is Premature," *UCLA Journal of Law & Technology* 8 (Fall 2004) (discussing how most fears concerning RFID use are exaggerated).

[53] Zhi Zhang, "Networked RFID Systems for the Internet of Things," Doctoral Thesis in Electronic and Computer Systems, KTH School of Information and Communication Technology Stockholm, Sweden, May 2013, www.diva-portal.org/smash/get/diva2:613266/FULLTEXT01.

[54] See Adam Thierer, "Lessons from the Gmail Privacy Scare of 2004," *Technology Liberation Front*, March 25, 2011, http://techliberation.com/2011/03/25/lessons-from-the-gmail-privacy-scare-of-2004.

[55] Letter from Chris Jay Hoofnagle et al. to Bill Lockyer, Attorney General (May 3, 2004), available at http://epic.org/privacy/gmail/agltr5_3_04.html.

[56] Dante D'Orazio, "Gmail Now Has 425 Million Active Users," *The Verge*, June 28, 2012, http://www.theverge.com/2012/6/28/3123643/gmail-425-million-total-users.

[57] See Kashmir Hill, "Apple and Google To Be The Whipping Boys for Location Privacy," *Forbes*, April, 26, 2011, http://www.forbes.com/sites/kashmirhill/2011/04/26/apple-and-google-to-be-the-whipping-boys-for-location-privacy.

[58] Brian X. Chen, "Why and How Apple Is Collecting Your iPhone Location Data," *Wired: Gadget Lab*, April 21, 2011, http://www.wired.com/gadgetlab/2011/04/apple-iphone-tracking (explaining how and why Apple uses location data, but pointing out that there was no known reason to keep phones' entire location history in an unencrypted file on the device).

[59] See Adam Thierer, "Apple, The iPhone And A Locational Privacy Techno-Panic," *Forbes*, May 1, 2011, http://www.forbes.com/sites/adamthierer/2011/05/01/apple-the-iphone-and-a-locational-privacy-techno-panic.

In a similar way, we are currently witnessing the development of social constraints on mobile phones in various environments. For example, the use of mobile devices in some restaurants and most movie theaters is frowned upon and actively discouraged. Some of these norms or social constraints are imposed by establishments in the form of restrictions on mobile device usage. Some establishments have even created incentives for compliance by offering discounts for those patrons who voluntarily check-in their devices.[60] Similar smartphone rules and norms have been established in other contexts. "Quiet cars" on trains are one example.

In other cases, these norms or social constraints are purely bottom-up and group-driven. For example, "phone-stacking" refers to a new social convention in which friends having dinner agree to stack their phones in a pile in the middle of the table to minimize distraction. To encourage compliance with the informal rule, the first person who touches their phone must pick up the check for the entire table.[61]

It is likely that similar social norms and pressures will influence the development of wearable computing technologies, such as Google Glass.[62] Already, numerous advice columns have been written about "Google Glass etiquette."[63] Suggested social etiquette includes: don't wear Google Glass when first meeting someone; immediately remove it when it is clear it is making others around you uncomfortable; take Google Glass off in bathrooms or other intimate and highly private settings; and only use its voice commands in public when really necessary. Again, many establishments already impose restrictions on the use of cameras and smartphones (such as their use in gym locker rooms) and those same rules will be applied to Google Glass or other wearable computing technologies.

The public will also expect the developers of IoT technologies to offer helpful tools and educational methods for controlling improper usages.[64] This may include "privacy-by-design" mechanisms that allow the user to limit or intentionally cripple certain data collection features in their devices. "Only by developing solutions that are clearly respectful of people's privacy, and devoting an adequate level of resources for disseminating and explaining the technology to the mass public" can industry expect to achieve widespread adoption of IoT technologies.[65]

More forceful opposition may develop to Google Glass and other wearable computing or recording devices. A group known as "Stop the Cyborgs" has already developed a website with various resources to push back against these technologies.[66] The group offers free downloadable "Google Glass ban signs" that can be displayed in places where such technologies are unwelcome.[67] They also offer stickers and shirts that convey the same message.

[60] Martha C. White, "Hang Up and Eat: Give Up Your Cell Phone and Restaurant Discounts Your Meal," *NBC News.com*, August 16, 2012, http://www.nbcnews.com/business/hang-eat-give-your-cell-phone-restaurant-discounts-your-meal-946635.

[61] Elie Ayrouth, "Phone Stacking—Is This the Next Phone Etiquette Dining Trend?" *Food Beast*, January 6, 2012, http://foodbeast.com/content/2012/01/06/phone-stacking-is-this-gem-of-social-engineering-the-next-dining-trend.

[62] Jared Newman, "The Real Privacy Implications of Google Glass," *Time Tech*, May 2, 2013, http://techland.time.com/2013/05/02/the-real-privacy-implications-of-google-glass.

[63] Kevin Sintumuang, "Google Glass: An Etiquette Guide," *Wall Street Journal*, May 3, 2013, http://online.wsj.com/article/SB10001424127887323982704578453031054200120.html; Rebecca Greenfield, "The First Rule of Google Glass Etiquette," *Atlantic Wire*, May 6, 2013, http://www.theatlanticwire.com/technology/2013/05/google-glass-etiquette/64916; Ryan Singel, "Devising a Personal Google Glass Privacy Policy," *Medium.com*, May 13, 2013, https://medium.com/future-participle/2334fecda87e.

[64] Shara Tibke, "Qualcomm Walks Fine Line between Privacy, Connected Devices," *CNet*, May 7, 2013, http://news.cnet.com/8301-1035_3-57583225-94/qualcomm-walks-fine-line-between-privacy-connected-devices (citing Qualcomm chief executive Paul Jacobs on the importance of companies figuring out a way to make IoT technology less intrusive).

[65] RFID Working Group, *Internet of Things in 2020*, 21.

[66] Stop the Cyborgs, "About," last accessed May 20, 2013, http://stopthecyborgs.org/about. ("'Stop the Cyborgs' was founded in response to Baidu eye, Google Glass, Life Logging and other technology trends including combination of the internet of things with big data. The aim of the movement is to stop a future in which privacy is impossible and where the iron cage of surveillance, calculation and control pervades every aspect of life.")

[67] Stop the Cyborgs, "Google Glass Ban Signs," last accessed May 20, 2013, http://stopthecyborgs.org/google-glass-ban-signs.

CONCLUSION

In the long run, if serious concerns develop because of inappropriate IoT uses, many federal and state laws already exist that could address perceived harms in this context. Property law already governs trespass, and new court rulings may well expand the body of such law to encompass trespass by focusing on actual cases and controversies, not merely imaginary hypotheticals. State "peeping Tom" laws already prohibit spying into individual homes.[68] Privacy torts—including the tort of intrusion upon seclusion—may also evolve in response to technological change and provide more avenues of recourse to plaintiffs seeking to protect their privacy rights.[69]

But policymakers should exercise restraint and avoid the impulse to regulate before serious harms are demonstrated. While it is true that "the impacts of this technology on society will be highly complex and likely unpredictable,"[70] that does not mean policymakers should attempt to anticipate and preemptively regulate every conceivable negative consequence of associated with the Internet of Things. All new technologies and innovations involve risk and the chance for mistakes, but experimentation yields wisdom and progress. A precautionary principle for the Internet of Things, by contrast, would limit those learning opportunities and stifle progress and prosperity as a result.

To reiterate, an "Anti-Precautionary Principle" is the better default here and would generally hold that:

1. society is better off when technological innovation is not preemptively restricted;
2. accusations of harm and calls for policy responses should not be premised on hypothetical worst-case scenarios; and
3. remedies to actual harms should be narrowly tailored so that beneficial uses of technology are not derailed.

Thus, we should continue to allow progress through trial-and-error experimentation—in other words, "permissionless innovation"—so that we can enjoy the many benefits that accrue from this process, including the benefits of learning from the mistakes that we will sometimes be made along the way.[71]

Finally, it is vital to remember that not everyone shares the same sensitivities as it pertains to online safety, security, and privacy.[72] Citizens also care about other many other values, including cost, convenience, and choice.[73] Preemptive regulation in this particular context is likely to overprotect privacy at the expense of those other values and retard the development of IoT technologies. Privacy itself is not a static value; it evolves over time in response to new developments and cultural norms and attitudes.

If we want the next great wave of Internet innovation to occur and for the Internet of Things to flourish, restraint and prudence should guide public policy in this context.

[68] For example, see Va. Code Ann. § 18.2-130, on peeping or spying into a dwelling or enclosure.

[69] Restatement (Second) of Torts §§ 652B (1977).

[70] BCS & Oxford Internet Institute, *Societal Impact of the Internet of Things*, 3.

[71] Adam Thierer, "Who Really Believes in 'Permissionless Innovation'?" *Technology Liberation Front*, March 4, 2013, http://techliberation.com/2013/03/04/who-really-believes-in-permissionless-innovation.

[72] Adam Thierer, "The Pursuit of Privacy in a World Where Information Control Is Failing," *Harvard Journal of Law & Public Policy* 36 (2013): 414–21, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2234680.

[73] Testimony of Adam Thierer before the Senate Committee on Commerce, Science and Transportation, Hearing on "A Status Update on the Development of Voluntary Do-Not-Track Standards," April 24, 2013, http://mercatus.org/publication/status-update-development-voluntary-do-not-track-standards.