THE INTERNET OF THINGS:

THE FUTURE OF LISTENING

GOODWIN PROCTER LLP

WHAT IS THE INTERNET OF THINGS?

The Internet of Things (IoT) conceptually refers to the dynamic networks that link physical objects with the virtual world via Internet connection, enabling "things" to sense, log, interpret and communicate information, as well as act autonomously or in cooperation with other devices, environments, and people.[1] IoT connected objects' computing power and connectivity may range from very limited to extensive, and types of sensors or data collection technology used will vary. The Internet currently connects anywhere from 10 billion to 16 billion objects;[2] even so, more than 99 percent of the estimated 1.5 trillion things globally remain unconnected.[3] By 2020, there may be anywhere from 26 billion to 50 billion globally connected objects.[4]

The proliferation of connected objects and embedded sensors will generate data in real time and across time and in volumes far beyond that seen to date. Just as the Internet to date has increased access to information, provided opportunities for collaboration, and stimulated economic growth, so too does the IoT present possibilities for a host of societal, economic, and personal benefits. When individual objects such as cars, roads, thermostats, refrigerators, medication-monitoring pills, fitness devices, or even livestock or migrating animals are equipped with sensors and the ability to communicate information that is tracked, they can become tools for understanding complexity and improving a process or user experience. The IoT offers a world where everyday objects can: "listen" to their environment, begin to recognize people's needs, personalize their environments, anticipate their behavior, and respond to their presence.

As a result, businesses can become more efficient, innovative, and attentive to their customers' needs and desires.

WHY DOES THE INTERNET OF THINGS MATTER?

Predictions of the IoT's global economic impact by 2020 range from $1.9 trillion to as high as $14.4 trillion via the combination of increased revenues and lower costs.[5] Component costs are expected to drop so low that connectivity will become a standard product feature,[6] and companies that do not try to harness the power of the IoT may be at a competitive disadvantage or find their products or services obsolete.

Already organizations are innovating IoT technologies and putting data they collect to use. For example:

- Cities and municipalities are collaborating with technology companies to develop intelligent traffic management systems with sensors that process traffic information, toll systems that vary prices based on traffic flows, and an advisory system to alert motorists to traffic jams or accidents.[7]

- Agribusiness is deploying predictive analytic tools to better gauge and manage weather and crop conditions, coordinate logistics, and improve food safety.[8]

- Businesses and consumers alike are using smart thermostats and lights to help save time and money and conserve energy,[9] and governments and utility companies are deploying smart grid technologies to improve energy efficiency.[10]

- Health companies are developing wearable or home health monitoring devices, medical applications, and even an ingestible sensor that can relay data to an application.[11]

The potential of the IoT is virtually limitless. But one thing is clear: enabling a world of efficiency, automation, innovation, and personalization requires the fundamental ability to listen. Just as speaking freely is often regarded as fundamental to communication, so too is listening. Organizations that seek to leverage the power of listening and recognize its importance for connected devices and smart tools must have the ability to collect, analyze, and process data in a trustworthy manner. Collectively, everything related to or arising out of the production and consumption of IoT goods and services can be referred to as the "listening economy."

WHAT LEGAL & PRIVACY CONCERNS ARE CREATED BY THE INTERNET OF THINGS?

While the IoT will likely generate substantial economic, social, and personal benefits, including more efficient use of time and resources, increased public and personal safety, improved health care, and increased opportunities for growth and innovation, it also generates legitimate privacy and legal concerns. To illustrate but a few concerns:

"Big Data" is an understatement. In the not so distant future, ubiquitous connectivity will enable listening and observation *at scale.* For consumers, this may mean that many aspects of everyday life that previously seemed private or invisible may now be discernible. Federal Trade Commission Chairwoman Edith Ramirez remarked recently that "[t]he enormous data trove that will result [from the Internet of Things] will contain a wealth of revealing bits of information that, when patched together, may present a deeply personal and startlingly complete picture of us."[12] This data may reveal an individual's identity, location, medical issues, religious or political preferences, financial information, family and friends, sexual orientation, favorite coffee shop, driving habits, whether her home's doors and windows are locked, and when she is not home. Put bluntly, we have always made noise as we interacted with the world around us, but soon that world will be much better equipped to listen and make sense of what it hears.

The importance of data security will increase. When digital material is incorporated into physical objects, those objects adopt all characteristics of digital technology—they become programmable, addressable, sensible, communicable, memorable, traceable, and associable.[13] They also become hackable. The public has just begun to appreciate the significance of securing a traditional network, but the game is already changing and networks are becoming anything but traditional. Seemingly innocuous devices like a refrigerator or bathroom scale may not appear to hold the keys to the vault, but bad actors often seek to exploit the easier opportunities for access before trying to break through the locked front door. If a refrigerator is connected to a home Wi-Fi network, it may open a back door to other devices and data on that network if appropriate safeguards are not put in place. Not only might sensitive information become vulnerable, but the risks of remote control and utilization of the devices themselves will increase. Connected devices that have already been hacked include pacemakers, insulin pumps, cars, door locks, baby monitors, ATMs, and cameras.[14] In virtually all of these cases, the hackers attempted to illustrate the feasibility of compromising the device's security controls. Beyond connected device security, strong data security protections for organizational databases will be ever more critical—consequences of a database breach could be more severe than just risk of identity theft or financial exposure. Nonetheless, data security must be balanced with usability—a door with 100 locks is very secure but may not be a very good door.

Traditional notice and consent may become unworkable. As disruptive practices and technologies evolve, so too must the related regulatory schemes that govern and seek to balance risks and benefits progress. Just as the expansion of cattle grazing, the railroad, and sales of goods required evolution of their initial or traditional governance principles, the rise of Big Data, the IoT, and the listening economy will likely herald the need for a progression in the regulatory approach to privacy and information handling. The Fair Information Practices (FIPs), which were originally developed in the 1970s at the dawn of

the Information Age, underpin many of the world's various privacy regimes. In particular, the FIPs' principle of "notice and consent" has become the dominant means for authorizing data collection and processing. "Notice and consent" generally requires that the individual whose personal data is being processed has been informed of the reason, context, and purpose of the collection and processing (*e.g.*, by posting of privacy policies) and has given consent (*e.g.*, via click-through consent mechanisms). As the IoT develops and we move fully beyond the era of desktop computing, notice and consent may become unworkable,[15] and pressure is likely to mount to establish default rules and systems that minimize the costs and consequences of respecting individuals' information-related preferences. For one thing, the IoT relies on a broad array of devices across countless locales, and the volume and velocity of information flows is likely to increase dramatically. If traditional notice and consent were to be required, individuals would be prompted to consent to data collection and use every time they encounter a new connected device—which could occur hundreds of times a day. Such a process would be incredibly burdensome.[16] Further, many connected devices will not be equipped with a user interface or may be entirely invisible to the consumer (*e.g.*, traffic sensors in a roadway, utility meters). As a result, new approaches to identifying and respecting information preferences will need to emerge as society adjusts to the risks and the benefits of the listening economy. Very real IoT privacy concerns will likely trigger serious public policy discussions regarding allocation of rights and responsibilities among "speakers" and "listeners." Choices will be made, and it seems likely that in any number of instances users of data—the proverbial "listeners"—will face restrictions intended to create enhanced accountability and sustainable patterns of data collection and use that strike a balance between the interests of individuals and the free flow of information [17]

The Future of Liability: What happens when things go wrong—and who is responsible? The IoT will generate new legal challenges and catalyze new thinking on the relationship between software and products liability. Historic warranty disclaimers and user expectations when the "network is down" or the product is "buggy" will increasingly be re-evaluated when the effect of such outages or performance issues begins to impact areas of life previously not directly affected by software. It is rare to find a piece of technology that functions perfectly all the time or in all conditions. Whether caused by software glitches, natural disasters, or aging, malfunctions or break downs will happen. The IoT will further complicate matters in two ways. First, things (and people) previously not reliant upon software will gradually be unable to function without it. Second, devices will increasingly depend on data to make decisions—data whose reliability may be suspect or even faulty (*e.g.*, the GPS that directs you to drive into a river). Futurists envision a world where devices can "think" and "sense" and respond automatically. If that GPS system is now directing a vehicle to drive automatically, what happens when the vehicle is directed to drive into the river? And if it drives into the river and the occupants (if there are any) or goods inside are harmed, who should bear legal responsibility—the vehicle owner, the GPS manufacturer, or the car manufacturer? And even if there is a manual-override to a technology, will the users even know how to use it or remember how to perform the function the device now carries out for them? The proliferation of the IoT could trigger a re-evaluation of technology-related legal norms as the potential costs and consequences of machine-managed decision making grow.

Smart data as evidence in criminal and civil litigation—gold mine or land mine? IoT data could provide a wealth of evidence that might make or break criminal investigations or civil suits (*e.g.*, whether a defendant was home at the time of the incident or what the driver was doing seconds before a crash). But such data will come with costs. Significant amounts of time *and* money will be spent grappling with discovery implications of data that many likely do not or will not consider discoverable, and systems will have to be built to accommodate the preservation and review of such information. What is more, problems of reliability and admissibility will likely plague the collection and use of such evidence. In the criminal context, use of IoT data raises constitutional questions relating to lawful searches and seizure under the Fourth Amendment, particularly with respect to individuals' reasonable expectations of privacy in their location information. Organizations that control IoT data or manufacture IoT devices are not immune from the potential financial and reputational costs, as they are likely to face increased requests for stored data from law enforcement, courts, and government entities.[18]

ADAPTING TO THE INTERNET OF THINGS: SOME PRACTICAL CONSIDERATIONS

Pragmatic organizations will seek to balance the values of privacy, security, free flow of information, and innovation. Greater system integrity and trust—which are proxies for reliability—will facilitate adoption and growth. Achieving this system integrity can be made easier through the use of the following principles and concepts:

- Recognize privacy and data security as differentiating features from the start. When developing new products and services, consider and plan for privacy and data security from the start. While this may increase initial outlay, many of these expenses can be addressed in a scalable manner that is directly proportional to the data-related risks that may arise.

- Embrace data de-identification and obfuscation tools. Many of the benefits of the IoT can be obtained through the collection, use, and retention of data in ways that acknowledge the sensitivity of information and actively seek to manage these concerns. De-identification and obfuscation not only create security-related benefits (both for the business and for consumers) but such techniques can also help create the peace-of-mind and consumer confidence that will be essential to the use and development of many new markets.

- Use relationship-dependent context to set appropriate defaults on information usage. Even if there may be unexpected new uses for data previously collected, businesses should ask the practical question: Is a proposed use consistent with or aligned with consumers' (or even the business') understanding of the nature and purpose for which the information was collected? In both the consumer and business worlds, especially in relation to machine-to-machine communications, businesses will increasingly be asked to put themselves in the shoes of their customers and ask hard questions about what is in those customers' best interests and what do or would those customers expect. More and more, consumers and industry will look to the law to allocate rights and responsibility in the listening economy.

- Embrace the benefits of transparency and clarity. As traditional notice and consent becomes less feasible, transparency about how data is collected and used becomes more important. Educating consumers about how data collected is used to benefit them or make decisions about them and what their rights, if any, are with regard to that data continues to be a way to soften any "creepiness" factor. Further, transparency and open approaches to data utilization will engender user trust. Because the amount of collected data is expanding so dramatically, many organizations will progressively turn to principles-based approaches to information management and governance. Rather than having long, detailed, heavily-lawyered notices, these organizations will turn towards values-based articulations of their information practices. This next generation of privacy will leverage the work of the Federal Trade Commission, financial institutions regulators, the Department of Health & Human Services, and practical experience to empower better privacy decision-making by business and consumers at much lower costs.

- Evaluate mechanisms to help ensure partner and vendor accountability. Increased connectivity may require or foster increased collaboration with other organizations, and services outsourcing is likely a secular market trend. While many organizations are already contractually obligating third parties that they work with to meet certain data privacy and security standards, the importance of this is increased by the IoT. Systems and organizations will evolve to enable greater collaboration and trust, but system integrity and reliability are critical components to support these advances.

- Identify existing processes that could benefit from the IoT. Brainstorm what types of new data could be useful to optimize operations and assets or improve service and safety and what new or existing equipment could be enabled with sensors to collect that data.

- Anticipate data-related infrastructure scalability. Enterprises are likely to see enormous amounts of data traffic coming from numerous sources. Those that proactively plan for this by building in appropriate bandwidth, storage capability, and application and device interoperability may find they have a competitive advantage in the market.

- Develop business continuity and disaster recovery plans and build in redundancies or fail-safes. Organizations that increasingly rely on IoT technology to automate or improve business processes should plan for the worst. It is also critical to understand how your product or service may interact with others to create unsafe or undesirable situations, and then strategize as to how to avoid such scenarios or build in fail-safe mechanisms.

- Assume someone will try to hack your device or service. Be responsive to consumer complaints and concerns, monitor internet forums and blogs for discussion of your device or service, and engage in rigorous testing so that when someone tries to hack your device or service or if someone discovers a vulnerability, you can respond promptly and thoughtfully.

- Consider IoT implications before new technology investments. Organizations can prepare by testing new IT products before they invest, considering how those products will adapt to the IoT, ensuring compatibility with existing systems with flexibility for future IT, and estimating their return on investment. Few companies can afford to completely overhaul their IT systems all at once. Combining forward-thinking expenditures with existing, immediate needs may ease some of the future growing pains of the IoT.

---

[1] The process of machines communicating with one another is also referred to as the Machine-to-Machine paradigm.

[2] Cisco Internet Business Solutions Group, *Embracing the Internet of Everything to Capture Your Share of $14.4 Trillion*, at 1-2 (2013), *available at* http://www.cisco.com/web/about/ac79/docs/innov/IoE_Economy.pdf (10 billion); Gil Press, "*Internet of Things By the Numbers: Market Estimates and Forecasts*," Forbes, Aug. 22, 2014, http://www.forbes.com/sites/gilpress/2014/08/22/internet-of-things-by-the-numbers-market-estimates-and-forecasts/ (16 billion).

[3] Cisco Internet Business Solutions Group, *Embracing the Internet of Everything to Capture Your Share of $14.4 Trillion*, at 1-2 (2013), *available at* http://www.cisco.com/web/about/ac79/docs/innov/IoE_Economy.pdf.

[4] *See, e.g.*, *Cisco Visualizations: The Internet of Things*, Cisco Internet Business Solutions Group, http://share.cisco.com/internet-of-things.html (last visited Sept. 4, 2014) (50 billion); Press Release, Gartner, Inc., *Gartner Says the Internet of Things Installed Base Will Grow to 26 Billion Units by 2020* (Dec. 12, 2013), *available at http://www.gartner.com/newsroom/id/2636073* (26 billion).

[5] *See, e.g.*, Peter Middleton, Peter Kjeldsen, and Jim Tully, *Forecast: The Internet of Things Worldwide, 2013*, Gartner, Inc., November 18, 2013 ($1.9 trillion); IDC, *The Internet of Things is Poised to Change Everything, Says IDC*, October 3, 2013, http://www.idc.com/getdoc.jsp?containerId=prUS24366813 ($9 trillion in annual sales); Cisco, *supra* note 3 ($14.4 trillion).

[6] Gartner, *supra* note 4.

[7] *See* Lopez Research, *Smart Cities are Built on the Internet of Things*, at 4-5, *available at* http://www.cisco.com/web/solutions/trends/iot/docs/smart_cities_are_built_on_iot_lopez_research.pdf.

[8] Ryan Huang, *Internet of Things: 5 Applications in Agriculture*, http://newsroom.hwtrek.com/?p=626.

[9] Chad Brooks, *The Internet of Things: A Seamless Network of Everyday Objects*, LiveScience (July 31, 2013), http://www.livescience.com/38562-internet-of-things.html.

[10] U.S. Dept. of Energy, Office of Electricity Delivery & Energy Reliability, *Smart Grid*, Energy.gov, http://energy.gov/oe/services/technology-development/smart-grid (last visited Sept. 4, 2014).

[11] *See, e.g.,* Nile Lars, *Connected Medical Devices, Apps: Are They Leading the IoT Revolution – or Vice Versa?*, Wired, Jun. 17, 2014, http://innovationinsights.wired.com/insights/2014/06/connected-medical-devices-apps-leading-iot-revolution-vice-versa/; Press Release, Proteus Digital Health, *Proteus Digital Health Announces FDA Clearance of Ingestible Sensor*, Proteus Digital Health (Jul. 30, 2012), *available at* http://proteusdigitalhealth.com/proteus-digital-health-announces-fda-clearance-of-ingestible-sensor/.

[12] Opening Remarks of FTC Chairwoman Edith Ramirez, *The Internet of Things: Privacy and Security in a Connected World,* at 2-3 (Nov. 19, 2013), http://www.ftc.gov/public-statements/2013/11/opening-remarks-ftc-chairwoman-edith-ramirez-federal-trade-commission.

[13] Stefanie Turber, Jan vom Brocke, et al., *Designing Business Models in the Era of Internet of Things*, *in* Advancing the Impact of Design Science: Moving from Theory to Practice 17, 21(Springer Int'l Publ. Switzerland, 2014).

[14] *See, e.g.*, Chris Poulin, *19 Amazing Hacks: Security Vulnerabilities That Cross the Physical Divide*, Security Intelligence Blog, IBM Corporation (Aug. 5, 2013), http://securityintelligence.com/19-amazing-hacks-security-vulnerabilities-that-cross-the-physical-divide.

[15] *See generally* Fred H. Cate & Viktor Mayer-Schöenberger, *Notice and Consent in a World of Big Data*, 3 Int'l Data Privacy Law, no. 2, 2013, at 67-73; Christopher Wolf & Jules Polonetsky, *An Updated Privacy Paradigm for the "Internet of Things,"* Future of Privacy Forum (Nov. 19, 2013), http://www.futureofprivacy.org/wp-content/uploads/Wolf-and-Polonetsky-An-Updated-Privacy-Paradigm-for-the-%E2%80%9CInternet-of-Things%E2%80%9D-11-19-2013.pdf.

[16] "It is unrealistic to expect that individuals will be willing or able to effectively register their informed preferences in a world where they are regularly prompted to read and accept notices of complex data collection, use, and sharing practices… Instead of protecting privacy, strict adherence to traditional notice and choice principles may drive individuals to give up." Wolf & Polonetsky, *supra* note 15, at 4-5.

[17] For detailed discussion of proposed privacy frameworks for an IoT world, s*ee supra* note 15.

[18] *See id.*

Contacts

Gerard M. Stegmaier, CIPP/US
202.346.4202
gstegmaier@goodwinprocter.com

Britanie Hall, CIPP/US
202.346.4061
bhall@goodwinprocter.com

About the Authors*

Gerard M. Stegmaier and Britanie Hall are attorneys at Goodwin Procter LLP, where they are members of the firm's Privacy & Data Security Practice. Mr. Stegmaier and Ms. Hall provide strategic counseling, advisory, and litigation expertise to emerging enterprises as well as Fortune 100 companies across a wide range of industries on Internet strategy, privacy, and data security. They have assisted numerous enterprises, founders, investors, and advisors with product launches and strategy, corporate and data licensing transactions, disclosures and marketing, regulatory compliance, litigation avoidance, and risk management.

**This article includes opinions of the authors and does not necessarily represent the views of Goodwin Procter LLP, its clients, or other organizations with whom the authors may be affiliated.*

GOODWIN
PROCTER