Bloomberg Law

Privacy and Security Law Report®

Internet of Things Privacy

For today's companies, navigating new paths to growth in the complex and evolving internet of things landscape requires innovative thinking and practical counsel. When it comes to a foolproof IoT roadmap, it is best to run a marathon, and not a race, to market, the authors write.

The Self-Driving Turtle Wins the Race: Managing the Privacy and Security of Fast-Paced IoT Innovation

BY JAMES H. KOENIG AND SHERRESE M. SMITH

As the internet of things (IoT) brings connectivity to virtually everything, it is changing the way we live, interact, do business and move through the world. The rapidly expanding quantities and types of data and the ways in which they are shared create a host of business opportunities, legal challenges and ethical questions. For today's companies, navigating new paths to growth in this complex and evolving landscape requires innovative thinking and practical counsel.

Jim Koenig is of counsel in the Privacy and Cybersecurity practice at Paul Hastings LLP in New York. Mr. Koenig has a business, technology and legal background and is a recognized authority on privacy, cybersecurity and data management issues.

Sherrese Smith is a partner in the Privacy and Cybersecurity practices at Paul Hastings in Washington. Smith has significant private sector and high-level government experience in media, communications, internet, digital technology and e-commerce issues as well as privacy, security and data security issues.

IoT by the Numbers

IoT refers generally to the ability of devices, vehicles, buildings, as well as everyday objects to connect to the internet and to send, receive and collect data. There is an explosion in the number of such devices—from smart homes and buildings, connected cars, medical devices, personal fitness devices, new payment systems and technologies and other exciting new products:

- The Federal Trade Commission reported that five years ago, the number of connected devices surpassed the number of people in the world.
- As of 2015, there were 25 billion connected devices worldwide.
- Gartner Inc. predicted a 500 percent growth by 2020.

We are increasingly surrounded by smart, connected devices. IoT includes everything from fitness wristbands to smart appliances. It pervades the energy grid, as well as machine-to-machine interactions in factories, data centers and hospitals. IoT devices and technology promise to free us from mundane tasks, communicate on our behalf without being asked and work tirelessly to boost our health, wealth, safety and security. IoT will enable new business models, and every business old or new will capture unprecedented volumes of data with

 ISSN 1538-3423

the potential to boost efficiencies and improve decision-making. IoT can simply change the fabric of our lives.

But along with these exciting promises come some serious risks.

Balancing Convenience With Privacy and Security (and Ethics)

The legal and practical challenges of IoT are less about the gadgets themselves and more about the unintended consequences of permitting them to gather our data and act as our agents. IoT risks show themselves in a variety of ways. For example:

Vehicles. Allowing a self-driving car to chauffeur us to work on the least traveled route may be a wonderful convenience until the day it takes us into a dangerous neighborhood or the software fails when we are unprepared to take the wheel or the car is taken over by a third party who has accessed the technology running the car. Sooner or later, a driverless car may cause a deadly accident, forcing the courts to decide whether the owner, the manufacturer or the software developer should be held responsible. From an ethics point of view, who programs the car's code to make a ''Sophie's Choice'' impact-minimization decision between fatally hitting another car with an elderly couple versus a child walking on the shoulder of a road?

Home. When you are near your home, the garage door opens, and the light and heat adjust to your preferred settings. The benefits are convenience and energy savings. Yet if improperly secured, the same technology could notify burglars in real time of your comings and goings, track your habits and predict when you will be away from home.

Buildings. By monitoring when people are in offices and the surrounding sun and weather conditions, smart buildings save energy by controlling lighting, heating and cooling, while improving physical safety monitoring. Without proper safeguards, however, monitoring systems may capture private, personal images. Employees in a relationship could find their privacy violated, and building owners could find themselves in possession of too much private information.

Urban Planning. Today's cities are always listening to and watching their citizens, which allows cities to provide beneficial services such as crime prevention and traffic control, but also conjures thoughts of ''1984.''

Medical Devices. Internet-based glucose pumps and heart pacemakers have helped patients better monitor and manage conditions. The Food and Drug Administration has established cybersecurity assessment standards, but attackers who found a flaw in that protection could weaponize these devices to stop someone's heart or deliver an insulin overdose.

The legal and practical challenges of the internet of things are less about the gadgets themselves and more about the unintended consequences of permitting them to gather our data.

These are not merely hypothetical, future threats. On March 17, the Federal Bureau of Investigation issued an alert to consumers to be aware of the cybersecurity risks of the computer technology already embedded in vehicles today. In July 2015, Chrysler recalled 1.4 million vehicles after security researchers demonstrated they could hijack the critical functions of a Jeep while it was driving down the highway. Similarly, cybersecurity researchers at the University of Michigan were able to hack into a smart home automation system giving the researchers the ability to unlock the front door of the home system being tested. Moreover, last month, a large number of smart devices from home internet routers and webcams connected via IoT were hijacked to mount one of the largest cyber distributed denial of service (DDOS) attacks that brought down some of the largest websites on the internet, including Twitter and others. While most such connected devices are often unprotected or less protected, a significant wide-scale vulnerability, imagine harnessing such massive, disruptive computing power against our own or foreign governments, to increasingly disrupt commerce or otherwise disrupt our personal lives.

A Three-Point Framework for Classifying IoT Risks

While many people fascinated or concerned about the ethics evolving around machine learning and IoT, innovators, entrepreneurs and lawmakers need a common lexicon to rationally discuss and manage IoT risk. From our various experience with clients, the most prominent privacy and security risks (and related analytics and machine learning) posed by IoT can be described in three broad risk categories:

Level 1: Direct Action/Reaction. IoT replaces a human action, like turning off the light when you leave the room or vacuuming a rug by an automated device that senses the boundaries of a rug or room.

Level 2: Delegated Decision-Making and Machine Learning. You tell your car: ''drive me home,'' and it takes a complex series of actions based on real-time traffic information, your learned routine and preferences, along with an understanding of physics, location and the rules of the road.

Level 3: Information Sharing With Third Parties and Device-to-Device Communications. Gathering and sharing the data with third parties to inform parents when children arrive home or to alert your favorite hotel chain you are on a business trip in the area. Also, the data is being shared device-to-device to inform better

  PVLR ISSN 1538-3423

autonomous decision making as well as tracking of devices, vehicles and people.

IoT innovators will have to continually ask: ''what could go wrong?''

Convenient, Creepy or Cool

Other questions to ask include ''how will consumers react?'' and ''how will regulators react?'' to your innovation. There is a fine line between what consumers consider convenient and what they consider ''creepy'' or an invasion of their privacy. Often the difference is whether they feel adequately informed, in plain language, about the trade-offs they are making. Regulators will also be watching how well you manage concerns like privacy and security of IoT.

Certainly, you need to understand what regulatory regimes are applicable to your product. For example, finding out that what you consider to be a sports wearable will instead be treated as a medical device—and therefore subject to much stricter controls—would be a rude surprise.

We may not be able to predict the reactions of consumers or regulators with absolute certainty, but we can mitigate the risks by following best practices.

How to Prepare—The Value of an Integrated Approach

Law and consulting firms that understand technology have helped clients through previous waves of technological change that led up to IoT. We can draw lessons from e-commerce, mobile payments, and other digital services, each of which raised its own thorny questions. The cybersecurity and personal privacy issues surrounding IoT are not so different from those surrounding the data generated by your social media or on-demand TV watching habits, which can be mined and analyzed for clues to your political, sexual and product preferences. The issue there is the same: access to data and insights never before available that can inform marketing and product development has the potential to be a minefield that can explode in a consumer and regulatory backlash, particularly with clumsy implementation.

The years 2016 and 2017 will be marked as the years where many companies start planning and employing new approaches to privacy and security to enable the future adoption, growth and promise of internet of things.

Despite the similarities, IoT is different enough to demand a much more integrated approach.

Because IoT innovations touch so many areas of the law, companies will also need access to multiple legal disciplines: patent protection, intellectual property, privacy and cybersecurity, regulatory compliance, litigation, financing, ecosystem agreements and more. With compressed product development cycles, companies will need to address all of these legal concerns at once.

IoT initiatives cry out for a combination of consulting expertise, legal discipline and knowledge of specific industries like automobile, medical device and consumer electronics manufacturing. For example, rather than relying on a lawyer's intuition about the use and misuse of data, the ideal team should include data scientists with a practical understanding of how data is collected, manipulated and correlated. Rather than merely standing ready to defend a company against a death or a data breach caused by a product flaw, the team should look for product safety and cybersecurity experts who can audit an implementation and spot those flaws prior to launch. Moreover, who are you going to call for guidance around the ethical implications related to IoT machine learning and use of derived data?

How to Build a Competitive Advantage—Five Next Generation Ideas for Next Generation Tech

For companies that want to build a competitive advantage in this space (or at least keep up), 2016 and 2017 will be marked as the years where many companies start planning and employing new approaches to privacy and security to enable the future adoption, growth and promise of IoT. Specifically, companies will have to update privacy notices/policies, third-party information sharing rights and contractual safeguards, and other key building blocks to incorporate the following five new concepts critical to achieve the full benefits of IoT as its technology and uses evolve:

1. Moving from Data Elements of Personal Information to Include ''Halo Data''

Most laws around the world define ''personal information'' using data elements of sensitive personal information (e.g., Social Security, credit card, bank account and debit card numbers), not necessarily the information created and used by IoT and monitoring technologies and derived with analytics. Yet, many companies have started to anticipate the next chapter of privacy and started identifying and managing ''Halo Data''—the data we generate as we move through, interact with and make decisions in the world around us.

2. New Notice and Choice Model for Range of IoT Decision Making

Industry is developing new models for notice and choice to explain the range of foreseeable actions and decisions and information sharing an IoT application/technology can take.

3. Curated Experience and the Agency of Permissions for Networks and Platforms

A new consent model allowing for agency of permissions to curated networks of trusted merchants, services and platforms that align with a person's specific preferences and comfort of IoT decision making and machine learning.

4. New Privacy Impact Assessment and Privacy-by-Design Approaches

Old and rudimentary approaches to privacy impact assessment and privacy-by-design will have to be overhauled to apply to IoT given the potential for constant monitoring, unintended consequences and uses of IoT information and the vast number of third parties that will be need to support an IoT advanced network.

5. Better Cybersecurity Vigilance

Enhanced cybersecurity by all players will be paramount as the privacy and safety of IoT users will depend on the safeguards of the weakest player as the backdoor into the IoT network.

Final Thoughts—How Not to Trip at the Finish Line

Innovators at the largest companies to the smallest startups are under pressure to move quickly. Product life cycles are only accelerating in the IoT era. Move too slowly, and opportunity will pass you by. Move too quickly, and the result could prove disastrous.

Ultimately, it's critical to take an integrated approach because a law firm may not know technology and a consulting firm may not know the legal risks. When it comes to a foolproof IoT roadmap, it is best to run a marathon, and not a race, to market.

PVLR ISSN 1538-3423