Secure the Refrigerator: Broad New California and Oregon IoT Security Laws Come Into Effect[1]

By Hywote Taye and Christine Lyon of Morrison & Foerster LLP

On January 1, 2020, California's landmark new Internet of Things (IoT) security law[2] took effect. The first of its kind in the United States, this law attempts to address growing concerns about protecting the security of everyday objects that connect to the internet (otherwise known as the "Internet of Things"). As the number of internet-connected devices expands seemingly endlessly, ranging across refrigerators, doorbells, alarm clocks, cars, vacuums, and so on, commentators have raised concerns about the security of these devices. In the U.S., California has taken the first step to address this concern legislatively, followed by Oregon, but it seems other states may not be far behind.

Who and what is covered?

The new California IoT security law applies to anyone who manufactures, or contracts with others to manufacture on its behalf, connected devices that are sold or offered for sale in California.[3] "The California law defines "connected device" as "any device, or other physical object that is capable of connecting to the Internet, directly or indirectly, and that is assigned an Internet Protocol address or Bluetooth address."[4]

Notably, this California law is not limited to consumer devices. The definition of "connected device" appears broad enough to cover even devices intended for industrial or other B2B purposes. This breadth appears to be intentional, as earlier drafts of the legislation would have limited the law to devices sold to consumers. Oregon's IoT law, which was modelled after California's and also came into effect in January, diverges in this respect, as it limits its definition of "connected devices" to devices that are "used primarily for personal, family or household purposes."[5]

It is also important to keep in mind that these California and Oregon laws are not limited to devices that collect or process personal information. Rather, their obligations apply broadly to any such devices that connect to the internet, regardless of what kinds of information they may process.

Both of these laws exclude providers of electronic stores, marketplaces, or other means for purchasing or downloading software.[6] They also provide limited exceptions for entities regulated by the Health Insurance Portability and Accountability Act (HIPAA), with respect to activity

[1] This article first appeared in CPO Magazine and is reprinted with permission.
[2] Cal. Civil Code § 1798.91.04 *et seq.*
[3] *Id.* at § 1798.91.05(c).
[4] Cal. Civil Code § 1798.91.05(b).
[5] ORS 646.607.
[6] Cal. Civil Code § 1798.91.06(b); ORS 646.607.

regulated by HIPAA.[7] Oregon's law also has an exception for activity regulated by the Food and Drug Administration with respect to medical devices.[8]

What is required?

Both California and Oregon laws require that connected devices be equipped with "reasonable security features."[9] According to both, the "reasonable security features" should be appropriate for the nature and function of the device; appropriate for the information the device collects, contains, or transmits; and designed to protect the device and any information contained therein from unauthorized access, destruction, use, modification, or disclosure.[10] Both states specify that a reasonable security feature may consist of a means for authentication from outside a local area network that has the following features: the preprogrammed password is unique to each device manufactured, or the device contains a security feature that requires a user to create a new means of authentication before accessing it for the first time.[11] Beyond this, neither provide clear guidance as to what else could constitute a "reasonable security feature."

What is next?

Other states have been actively considering similar laws, including bills proposed in New York and Virginia. Although California's Consumer Privacy Act (CCPA) has absorbed the attention of many businesses, it will be important for covered manufacturers to pay sufficient attention to this separate trend of expanding IoT security laws as well.

[7] Cal. Civil Code §§ 1798.91.06(h), 1798.91.06(d); ORS 646.607. California also excludes activity regulated by its own health privacy law. Cal. Civil Code § 1798.91.06(h).
[8] ORS 646.607.
[9] Cal. Civil Code § 1798.91.04(a); ORS 646.607.
[10] *Id.*
[11] Cal. Civil Code § 1798.91.04(b).

Compliance in a Connected World: Privacy and the Internet of Things[12]

By Mary Race and Christine Lyon of Morrison & Foerster LLP

The Internet of Things (IoT) is rapidly expanding. Our homes, cars and workplaces are filling with connected devices designed cater to our personalized needs. They respond to our instructions, whether delivered through a mobile app or a spoken command, and they collect data about our activities in order to better anticipate our needs. All of this data collection creates a digital trail of consumers' lives, which becomes richer and more detailed as multiple sources of data are combined. Big data analytics offers seemingly endless opportunities to use and commercialize this data in new ways.

Yet unanticipated uses and disclosures of user data may compromise consumer privacy and even undermine consumer trust. As a result, companies will need to pay increasing attention to privacy compliance in the IoT space, as courts and regulators focus on issues such as notice, choice, and security.

The FTC's settlement with the smart TV manufacturer Vizio, Inc. highlights several key privacy compliance challenges facing companies in the IoT space. In the settlement, which included a hefty payment of $1.5 million, the FTC reiterated its position that collecting and using information in ways that surprise consumers—such as Vizio's collection and sharing of consumers' television viewing activity via its connected televisions—requires "just-in-time" notice and choice. In addition, the FTC expanded its view of what constitutes sensitive personal information to include consumers' television viewing activity, an indication that regulators are willing to look beyond traditional concepts of personal information as they evaluate new types of data collected by connected devices.

Security and data protection concerns loom large in the IoT space. As devices become more connected and hackers become more sophisticated, companies developing IoT products will want to stay on top of data security, ideally by building sufficient protections into their product design. Current best practices, such as conducting privacy impact assessments of new products and services, are rapidly becoming legal requirements. When the European Union's General Data Protection Regulation took effect in 2018, for instance, companies developing IoT products became legally required to conduct data privacy impact assessments of technologies that involve consumer profiling or large-scale processing of sensitive information.

Companies should also be aware of privacy compliance issues that arise when employees interact with IoT in the workplace, such as through GPS-enabled devices that allow employers to track employee movement and location. At least one employer has been sued for requiring employees to install a smartphone app that allowed the employer to monitor the employees' location around the clock, even during non-work hours. Companies should strive to give proper

[12] The original version of this essay first appeared in Corporate Compliance Insights and is reprinted with permission

notice to employees, be thoughtful about collecting only the data they need, and consider how long they maintain the data.

The fact that precise location data is considered sensitive both in the U.S and internationally is particularly relevant in the IoT space. In an FTC action brought against the developer of a mobile flashlight app, for example, the agency alleged that the company deceptively failed to disclose that the app automatically transmitted a user's precise location and unique device identifier to third parties. The FTC ordered the company to provide a just-in-time notice and obtain opt-in consent for such data collection and sharing, including disclosures regarding how the location data may be used, why the app is accessing location data, and which third parties receive the location data directly or indirectly via the app.

Going forward, companies can expect to see expanding definitions of what types of data are considered personal information, legal battles over when and how law enforcement agencies can access user data, and industry self-regulatory initiatives to try to strike an appropriate balance between privacy and innovation. In an era of constant technological development, privacy compliance in the IoT space remains an ongoing challenge, while at the same time presenting an area of opportunity for companies that take privacy concerns into account when developing their products and services.

The Unblinking Eye: Employee Monitoring in the IoT Era[13]

By Christine Lyon of Morrison & Foerster LLP

The privacy concerns raised by the Internet of Things (IoT) have focused mostly on the consumer, whose personal data is captured in a growing list of goods, including mobile devices, fitness trackers, cars, and home appliances.

Less attention has been paid to the privacy of employees interacting with IoT in the workplace. For ample reasons, innovation in so-called industrial IoT (IIoT) is projected to explode in coming years. With the latest technologies, companies can better manage and track their inventory; automatically spot and service equipment failures; create safer work environments; and improve employee efficiency. These improvements are made possible through real-time communication between machines with software that collects and interprets vast amounts of data.

But companies investing in these technologies should be aware of potential legal-privacy risks that await. Even if it's not their primary function, many IIoT applications could be used to monitor employees in unintended ways. Use of such data, if it's not obtained properly, could damage a company's reputation or put it on the defense in litigation.

Take, for example, sensors that some industrial companies embed in employee uniforms and helmets. These kinds of sensors can detect hazardous conditions such as toxic gases, or warn of over-exertion based on the reading of an employee's heartbeat. Or consider GPS-enabled devices or mobile applications that permit employers to track the precise physical location of workers in order to deploy them most efficiently to new work assignments.

But what if information gleaned from these devices was used to detect patterns about an employee's movements, which could be used to draw negative conclusions about the employee's efficiency or performance? Yet an employee's slow pace in moving between work stations, or frequent departures for bathroom breaks, might be due to a legally protected medical condition rather than laziness. Penalizing the employee based on this data might set the employer up for a disability discrimination claim. Similarly, an employer may face whistleblower or retaliation claims if a manager is able to use location data to figure out which employee went to the human resources office to lodge a complaint about him or her. It is inevitable that employers will seek to use IoT data to better manage their employees, as well as their inventory and equipment, but employers will need to guard against inappropriate or even unlawful uses of this data.

The sensors do not need to be carried by the employees to raise potential privacy concerns. In a connected workplace, data about employees can be captured in any number of ways. Sensors connected to equipment -- forklifts, for instance -- could provide detailed information about an employee's movements. Again, harvesting and using this data could open up a Pandora's box.

Unfortunately, a myth persists that an employee's privacy rights end the moment he or she walks through an employer's door. The reality is more nuanced in the United States, where employees

[13] This article first appeared in Information Week and is reprinted with permission.

can and do bring claims against their employers alleging that monitoring activities invade their privacy, especially when the monitoring is high-tech or unexpected. And the myth is fundamentally wrong in places outside the United States, such as in Europe, which views privacy as a fundamental human right that follows employees into the workplace and thus imposes broad restrictions for monitoring employees.

Other stakeholders may have a say in employee monitoring as well. Unionized employers will need to consider their potential obligations to consult or bargain with the labor unions over employee monitoring programs. Employers will also need to assess their obligations under local employment laws to consult with works councils or other employee representatives and potentially to register with (or even seek approval from) local data protection authorities of certain employee monitoring activities. Employee monitoring activities that may be permissible in one country may be problematic in another, so it is important to consider local laws and practices.

To reduce the risk of employee claims and reputational harm, companies should keep a few best practices in mind:

- **Give proper notice to employees**. Office workers are used to receiving privacy notifications from their employers when they log onto their work computer. Similar notifications should be given to employees who are interacting with the IIoT.
- **Be thoughtful about what you collect and collect only what you need**. In seeking to improve workplace efficiency and safety, it's natural to want more data. The richer the data, the better the conclusions can be made about what needs improvement. But the more data collected, the more likely you could run into unforeseen legal consequences. Generally, when deciding what information to collect, make sure there is a strong business case that outweighs privacy concerns for individuals. In court, it's harder to defend data collection seen as excessive.
- **Be thoughtful about how long you maintain the data**. With data storage so cheap, it may be tempting to keep data for extended periods of time. But again, the longer you keep data, the more potential for legal risk. If maintaining data for long periods is critical, think about aggregating data so it's no longer personalized.