What’s trending on NP Privacy Partner

Internet of Things legislation in California halts, FTC recognizes measures to enhance Internet of Things device security, and Oregon joins the nationwide movement to prohibit employers from asking applicants about their prior salary history. Here’s what’s trending in data privacy and cybersecurity.

Consumer Privacy

Internet of Things legislation in California is dead for this year, but it will be back

The sponsor of “Internet of Things” privacy legislation in the California Senate has tabled the bill for the remainder of 2017, but remains committed to reactivating it in the second half of the 2017–2018 session. SB 327, introduced in March 2017, was prompted by a children’s internet advocacy group that was upset over toys, like the now-notorious Cayla doll, that have the ability to monitor the children with whom the toys interact and record their words and voice patterns, and potentially even the ability to transmit data from the children back to the Internet for marketing or other purposes. The sponsor of the bill referred to it as the “teddy bears and toasters” law.

The bill as originally introduced applied to any device capable of connecting to the Internet, and would have required point-of-sale disclosure as to a device’s capability to collect audio, video, location, biometric, health or “other personal or sensitive user information.” It also required disclosure as to how a consumer can obtain the privacy policy related to the use of such data, and required that security measures be in place for any such data, including notifications to consumers as to how to obtain updates and patches for such security measures. It also required that such a device be designed to communicate by “visual, auditory or other indicators” the fact that it is collecting data, and obtain user consent at the time of collection, unless such data collection was an implicit part of the device performing its “stated function.” Later, the bill was amended to limit its scope by specifying that it would only apply to household devices; that it only applied to video, voice or biometric/health information; that it did not apply to the auto industry; and that it did not limit law enforcement’s use of such data.

The hearings held on the bill in the Senate Judiciary Committee in May 2017 were marked by broad support for the idea of giving consumers control over data collection from their household devices, especially with regard to children’s toys, but also great unease that the topic of data collection by connected devices was so large, and so ill defined, that rushing through a bill after one hearing, with minimal input from industry, was bound to result in negative unintended consequences. The bill squeaked out of committee on what is known as a “courtesy vote,” which kept the bill alive so that...
more hearings could be conducted and additional refinements made. As a result, there is every likelihood that the bill will be taken up again in 2018.

The debate over SB 327 provides a taste of the questions that will confront legislators at the state or federal level as they grapple with the issue of how to regulate privacy in the “Internet of Things.” Should regulation apply only to consumers or to all of a product’s users? Who is the consumer of such a product anyway? Is point-of-sale notice of data collection capabilities useful? How can notice of data use be updated if the sort of data collected, or the purpose for which it is collected, changes after the device is in operation? How realistic is it to expect a device to constantly disclose to its user (or those in the vicinity) what data it is being collected and for what purpose? Won’t that result in a flood of meaningless over-disclosure? Is it realistic to expect users to constantly manifest their consent or lack of consent? If consent is deemed given for a device to collect the sort of data essential to its intended function, are there ambiguities inherent in the concept as well? What if different users perceive its essential function differently? And who is the owner of such data, for the purpose of applying existing data security and data breach laws? In addition, privacy concerns regarding the Internet of Things tend to be much broader in scope than existing data security and breach statutes, which are focused more on identity theft and medical data than the risks of lifestyle and consumer preference tracking.

One senator—who actually voted in favor of the bill—stated that his tax reform committee has conducted over thirty hearings with respect to the issues before it, and the interrelationship of privacy and the Internet of Things might turn out to be just as complicated. – Karl D. Belgum

---

**FTC provides comments on measures to enhance Internet of Things device security**

The Federal Trade Commission has submitted public comments to a working group convened by the U.S. Commerce Department’s National Telecommunications and Information Administration (NTIA), which is developing guidance about methods for Internet of Things (IoT) manufacturers to inform consumers about security upgrades for devices. In late April, the NTIA sought comments on its draft of Communicating IoT Device Security Update Capability to Improve Transparency for Consumers (“Elements of Updatability”).

The FTC bases its comments upon its law enforcement, policy initiative and consumer and business education. The FTC noted that the burgeoning IoT marketplace offers enormous benefits to consumers, such as health tracking data, real time notifications in connected cars and efficiencies in home utilities. Yet, the FTC warns that “consumers do not trust IoT devices,” which can create opportunities for attackers to steal data or assume device control by ransomware or botnets. In deciding whether and how to patch devices, manufacturers must balance the benefits of the enhanced safeguards against the costs of developing, testing and deploying software updates. Providing consumers with clear information about whether, for how long and at what costs their IoT devices will receive security support will benefit consumers, enhance competition and promote innovation.

The FTC commended NTIA for creating a multi-stakeholder process in which industry, government and consumer representatives have shared recommendations on enhancing IoT security. The Elements of Updatability divides its guidance into two categories: (1) “key elements” that IoT manufacturers should convey to consumers before sale to them to facilitate informed
purchasing decisions and (2) “additional elements” manufacturers should communicate to
consumers either pre- or post-purchase.

The “Key Elements” suggest that companies should make the following three disclosures before
sale: (1) whether the device can receive security updates, (2) how the device receives security
updates and (3) the anticipated timeline for the end of security support. The FTC recommends
adjusting the third disclosure (timeline) and adding a fourth one (key use limitations). The FTC
suggests that manufacturers should consider whether they can disclose a minimum support period
in addition to, or instead of, and an anticipated timeline. Disclosure of a guaranteed minimum
period would provide clear information to consumers as they compare devices. Also, the FTC
recommends adding to the “Key Elements” a disclosure of whether a device will stop functioning or
become highly vulnerable when security support ends.

Regarding the “Additional Elements,” the FTC recommends suggestions regarding information
that manufacturers should convey to consumers before or after purchase: (1) adopting a uniform
notification method (e.g., a standard position on the device’s screen or in the notification center of
the device-related app); (2) enabling consumers to sign up, either at the point-of-sale or after, for
affirmative notifications about security support; and (3) providing consumers with real-time
notifications when support is about to end. Finally, the FTC recommends the omission of the
“additional element” describing how the manufacturer secures updates and the update process.
Explaining those safeguards to consumers imposes significant communication costs on industry
while providing little, if any, benefit to consumers.

We will continue to review guidance documents and recommendations on the evolving security
and consumer issues arising with the proliferation of IoT devices. – Steven M. Richard

Employee/Workplace Privacy

Oregon latest jurisdiction to prohibit employers from asking applicants about their
prior salary history

The state of Oregon is the latest to join the nationwide movement to prohibit employers from
asking applicants about their prior salary history in connection with its legislative efforts to
eliminate pay disparity. While provisions in existing law already prohibited pay disparity between
“the sexes,” on June 1, 2017, Governor Kate Brown signed into law House Bill 2005, otherwise
known as the Oregon Equal Pay Act of 2017 (“the Act”). The Act significantly expands the scope of
pay disparity protections afforded to applicants and employees pursuant to Oregon law. The final
version of the Act passed both the Oregon senate and house unanimously, garnering tremendous
bipartisan support.

The Act outlaws discrimination “between employees on the basis of a protected class in the
payment of wages or other compensation for work of comparable character.” This extends the
protections of the Act to employees regardless of their race, color, religion, sex, sexual orientation,
national origin, marital status, veteran status, disability or age.

Importantly, the Act prohibits employers from seeking the salary history of an applicant or
employee from the employee or his or her current or former employer. An employer is, however,
permitted to request from a prospective employee an authorization to confirm prior compensation
after making an offer of employment that includes an amount of compensation. The law also
prohibits employers from screening job applicants based on current or past compensation or
determining compensation for a position based upon an applicant’s current or past compensation. This is not, however, intended to prevent an employer from considering the compensation of a current employee during a transfer, move or hire of the employee to a new position within the same employer.

Further, the Act permits employers to pay employees different compensation for comparable work if the difference in compensation is due to a bona fide factor related to the position and is based on (1) a seniority system, (2) a merit system, (3) a system measuring earnings by quantity or quality of production, (4) workplace location, (5) travel (if necessary), (6) education, (7) training or (8) experience.

Employers who violate the Act may be subject to complaints made by applicants or employees to the Oregon Bureau of Labor and Industries or private civil lawsuits. The Act, however, provides a number of employer defenses, including conducting an “equal pay analysis” of the employer’s pay practices that can be utilized to limit exposure.

Most of the provisions included in the Act will become effective between the fall of 2017 and January 1, 2019. Employers covered by the Act should review their applications and hiring practices now and reach out to local employment counsel to ensure timely compliance with the Act. – Christopher G. Gegwich and Alexander E. Gallin

For more information, please contact:

— Karl D. Belgum at kbelgum@nixonpeabody.com or 415-984-8409
— Alexander E. Gallin at agallin@nixonpeabody.com or 516-832-7548
— Christopher G. Gegwich at cgegwich@nixonpeabody.com or 516-832-7606
— Steven M. Richard at srichard@nixonpeabody.com or 401-454-1020

NP PRIVACY PARTNER BLOG
Staying ahead in a data-driven world: insights from our Data Privacy & Security team.