Bloomberg Law

Privacy and Security Law Report®

Consumer Data

The Machines are Talking–So Can We Sue Them If the Conversation Leaks?

Machine Liability

Machines have been helping people record, communicate, and listen for some time now, and in the process automatically collecting and storing mountains of data. As information is shared between machines and devices and becomes vulnerable to data breaches, can machines be considered negligent and manufacturers held liable for internet of things breaches, the author asks.

BY JASON R. SCHEIDERER

Your fitness tracker, in direct communication with your refrigerator, calculates that nearly all of your steps last Saturday were back and forth to the refrigerator. A simple example, and you might be annoyed that these machines have this information about you. But what if this information left the privacy of your home? What if this information left these two machines and became known to your personal trainer, or worse yet, was posted to your Facebook Inc. page? What if this information was released to your health insurance or life insurance carriers? And what if the information released was much more sensitive?

We have asked our machines to follow us, record us, listen to us, and communicate for us. In doing so, we have also asked the machines to create mountains of new data. All of this data is being saved, tracked, and shared in ways we may have never imagined, or wanted. We know we are being watched, but who is watching the watchers? Who (or what) is responsible for safeguarding the private information held by our machines and devices? And when things go badly, who is responsible?

Jason R. Scheiderer is a partner at Dentons LLP in Kansas City. Scheiderer is a member of the litigation and dispute resolution group, and the privacy and cybersecurity group.

The ''Internet of Things'' (IoT) is shorthand for the increasing variety of direct internet-based communication between machines. As information is shared between devices and machines, it is subject to many of the same threats of hacking and data theft. So can a machine be ''negligent'' in its data security ''practices?'' And if so, should the manufacturer be liable for a resulting data breach?

These questions lead us to the new frontier of data breach litigation and regulation. This article discusses recent lawsuits seeking to introduce these type of liability theories, notes early efforts by legislators and regulators to impose standards on IoT businesses, and provides recommendations for companies engaged in IoT business.

Litigation is Coming

''Data theft,'' ''data breach,'' and ''privacy invasion''—many lawsuits today invoke these terms. Data breach class action litigation has expanded significantly in recent years—in the number of suits, the number of potential class members, and in the scope of the alleged harm. Until very recently, the targets of these lawsuits have been consumer-facing businesses. Plaintiffs have typically asserted that a business failed to ad-

 ISSN 1538-3423

equately safeguard company data, allowing it to be taken from the company.

But when data stored or communicated by devices is hacked, who should be liable? The manufacturers of the machines that had access to the data? The network provider that connected the machines? The software developers whose software was deployed into the machines? For many plaintiffs' lawyers, the answer may be: all of them, at least until discovery can sort out their various roles.

In recent months, the plaintiffs' bar has begun pursuing class action liability theories against a variety of businesses involved in device connectivity.

Undisclosed Collection of Data A recent class action lawsuit against Vizio resulted in a $2.2 million settlement (the case was filed in the U.S. District Court for the District of New Jersey). Plaintiffs alleged that the Vizio's ''smart'' televisions were collecting too much customer information. Vizio was accused of tracking viewers' habits and preferences and secretly storing and transmitting that data. As part of the settlement, Vizio agreed to stop tracking viewers and to obtain informed consent for information collected in the future.

Standard Innovation was sued in 2016 because its ''We-Vibe'' vibrator product and its corresponding smartphone app did not inform users about the data it was collecting (the case was filed in the U.S. District Court for the Northern District of Illinois). The data included how often and how long users enjoyed the toy, the selected vibration settings, the device's battery life, and even the device's temperature. All of this data was collected and sent to the company's Canadian servers. The class action plaintiffs alleged that the company's undisclosed collection and transfer of data violated Illinois' consumer protection laws and the federal Wiretap Act. The lawsuit settled in March 2017, with final compensation to be determined and a final hearing set for later this year.

Data Vulnerability In *Cahen v. Toyota Motor Corp.*, plaintiffs alleged that the car manufacturers equipped their vehicles with computer technology that is vulnerable to hacking. Plaintiffs assert that a hacker can communicate remotely with the network of computers controlling many of the vehicle's functions, which could result in the driver losing control over the steering, acceleration, or braking systems. The plaintiffs claimed that the manufacturers were aware of these security vulnerabilities, but still marketed their vehicles as safe. Plaintiffs thus claimed that the manufacturers misrepresented known facts, and breached implied and common law warranties. The case is currently on appeal before the Ninth Circuit.

In *Flynn v. FCA US LLC*, plaintiffs alleged that there was a security flaw in the ''infotainment'' centers, which were installed in certain Dodge vehicles. The complaint asserts that the infotainment system is highly vulnerable to hacking, and, if hacked, could allow the hackers to take control of the car's steering, acceleration, and braking. The complaint similarly asserted misrepresentation and breaches of warranties.

VTech was called to answer for alleged vulnerabilities in its learning toys for children (the case is pending in the U.S. District Court for the Northern District of Illinois). The toys link to the internet to collect and receive data. However, plaintiffs claimed that a hacker defeated VTech's security measures and obtained customer data from the devices and web services. This information included pictures, chat logs, emails, passwords, and nicknames—often belonging to children. Plaintiffs alleged breach of contract, breach of the warranty, and violations of state consumer protection laws. Similar to the plaintiffs in the automobile cases, the plaintiffs alleged an increased risk of harm and that the value of the products had diminished.

Finally, in *Ross v. St. Jude Medical Inc.*, plaintiffs' claims arose out of medical devices—including pacemakers, defibrillators, and heart resynchronizers—that communicate using radio frequency wireless technology (the case is pending in the U.S. District Court for the Central District of California). The implanted devices' ability to communicate wirelessly allows them to be monitored remotely with in-home equipment. Plaintiffs claim that the devices and the in-home transmitters lacked ''basic security defenses,'' making them highly vulnerable to hackers.

In each of these cases, actual injury and standing has been an issue. These challenges mirror the ongoing battles in typical consumer data breach cases, where plaintiffs are challenged to prove actual injury based upon the risk that compromised data will be used to commit identity theft and other fraud in the future.

Plaintiffs, up to this point, have most often asserted legal claims arising out of an exposure to increased risk, the misrepresentation of risk, or the misrepresentation of data collected. But it will not be long before plaintiffs come forward with allegations of substantial injuries as a result of a breach of data security within a device. The consequences of a data breach in certain applications, such as industrial machines, automobiles, home security systems, and medical devices, could be catastrophic. Despite improvements and innovations in the industry, we can expect an increase in class action lawsuits and significant damages awards against manufacturers and other businesses within the IoT supply chain.

Regulatory Efforts

Federal Regulation Many governments—from small cities to multi-national pacts—have enacted data privacy regulations. Recently, several U.S. governmental bodies have turned their attention to IoT data security.

In 2015, the United States Federal Trade Commission (FTC) issued a staff report entitled, ''The Internet of Things: Privacy and Security in a Connected World.'' This guidance memorandum provides information for consumers, legislators, and businesses, encouraging best practices for IoT businesses. The FTC complemented its staff report with additional information directed more specifically at businesses in the IoT sector entitled, ''Careful Connections: Building Security in the Internet of Things.''

Among the key best practices currently recommended by FTC:

- devices should have security built into them at the outset (often referred to as ''security by design'' or ''security by default'');
- companies should conduct privacy or security risk assessment on new products or innovations;
- companies should minimize the data they collect and retain;
- companies should appropriately test their security measures before launching their products;

  PVLR ISSN 1538-3423

■ companies should provide clear notice of the ways in which the machine will collect and use data; and

■ companies should provide consumers and users with meaningful opportunities to exercise choices regarding their data.

The FTC is not alone in its focus on IoT data security. The National Institute of Standards and Technology, which is the federal agency that issues standards for government work, has created a program to assist businesses, particularly government contractors with IoT security.

Similarly, the Food and Drug Administration (FDA), the Department of Defense (DoD), and the Federal Communications Commission (FCC) have all recently included IoT-specific recommendations in their cyber-security standards and publications, each with their own priorities. The FDA is understandably very concerned about connected medical devices, the DOD has focused on standards for defense contractors, and the FCC includes IoT issues as part of its larger approach to consumer cyber-security.

While careful businesses proactively review statements, guidelines, and publications, enforcement actions seem to capture much more attention. Currently, the FTC does not have any specific rulemaking procedures to set minimum security practices for manufacturers or retailers. However, that has not eliminated the possibility of IoT security enforcement actions. Instead, the FTC has recently worked to enforce data security practices in the IoT sector through enforcement of promises made by manufacturers in their product websites, brochures, and advertising. FTC enforcement actions thus often allege unfair and deceptive practices under Section 5 of the FTC Act.

In January 2017, the FTC brought such an enforcement action against a computer networking equipment manufacturer, D-Link Corporation. The FTC asserted that the company had failed to undertake ''reasonable steps'' to secure wireless routers and IP cameras from ''widely known and reasonably foreseeable'' risks. The FTC claimed that the company was aware of ''well-known and easily preventable security flaws,'' which left consumers vulnerable to data privacy and security risks.

Given the stakes of data breach and the exponential growth of device connectivity, businesses should expect additional publications, recommendations, rule-making, and enforcement in the coming months.

State Regulation As many expected, California introduced one of the first efforts to mandate ''security by design.'' In 2017, a new bill (Senate Bill 327) was proposed that would require manufacturers and sellers of IoT connected devices to:

■ equip the device with ''reasonable'' security features, appropriate to the nature of the device and the information it collects, contains, or transmits;

■ design the device to indicate to the consumer when it is collecting information;

■ obtain consumer consent before the device collects or transmits information;

■ provide an explicit privacy notification to the consumer about what data is collected by the device; and

■ directly notify consumers of security patches and updates intended to make the device more secure.

Beyond manufacturers, the bill would also require retailers to provide a short, plainly written notice of the device's information-collection functions. This notice must be provided to the consumer at the point of sale. Specifically, the notice must inform the consumer whether ''the device is capable of collecting audio, video, location, biometric, health, or other personal or sensitive consumer information.'' Finally, the notice must tell the consumer where to find the device's privacy policy.

If this bill becomes law, California would be the first state able to bring enforcement complaints against companies that do not build proper security safeguards into their devices from the moment they are created. To date, companies have been encouraged to ''patch'' or to upgrade security when vulnerabilities are found, and industry groups have developed their own ''best practices.'' But California's effort would be the first codification of ''security by design.'' This concept requires manufacturers—from the earliest manifestations of the product—to plan and implement data security structures within the machine.

The Future

Right now, it is estimated that more than six billion devices and machines are connected to the internet in some form. By 2020, experts predict that there will be 50 billion internet-connected devices. As a result, by 2025 these connected devices will have an economic impact of more than four trillion. Put simply, device connectivity is prevalent now, and will become nearly ubiquitous in just a few years.

We know the machines will be creating, storing, and transferring data about us. And we know that some of this data will be personal, private, and sensitive—from our medical data to our finances. Right now, lawyers—from legislators to litigators—are searching for practices that will support the convenience of device connectivity while protecting privacy. Businesses large and small will be impacted by the legislation and liability theories that are created and implemented over the next few years.

Technology and trends continue to evolve, but there are certain practices and efforts IoT businesses should consider, including:

■ audit and regularly monitor user data already collected and purge unneeded data;

■ develop a data collection and storage procedure for user data going forward;

■ for new products, integrate physical security into product design at the earliest stage possible;

■ for new products, integrate software security into product design at the earliest stage possible;

■ develop and update notices to users regarding data collection and processing;

■ develop and deploy user-consent measures, such as waivers, ''click-wrap,'' and assumption-of-the-risk statements;

■ update and verify the accuracy of privacy disclosures and policies, both business-to-consumer and business-to-business;

■ implement a comprehensive testing, updating, and patching process for already released devices;

■ consider liability-shifting provisions in their agreements with vendors and administrators of the connectivity; and

■ consider insurance products that could provide necessary coverage.

When must manufacturers impose security apparatus into the devices they invent? What needs to be imbedded into the machine? What happens when a manufacturer fails to install ''appropriate'' security structures? What responsibility do retailers and resellers have for the machine's vulnerabilities—whether known, unknown, disclosed, or undisclosed? And how far should liability extend? These are the types of questions now posed by the tremendous growth and success of machine-based internet communication. Businesses should stay engaged in the analyses and developments that will shape our increasingly connected future.

BY JASON R. SCHEIDERER

To contact the editor responsible for this story: Donald Aplin at daplin@bna.com

PVLR ISSN 1538-3423