MAYER·BROWN

ELECTRONIC DISCOVERY & INFORMATION GOVERNANCE

Tip of the Month

ESI Discovery Challenges of the Internet of Things

Scenario

A US consumer products manufacturer plans to launch a line of smart products for the kitchen ranging from coffee makers to refrigerators capable of gathering data on customer use and performance that will be used to improve the user experience. Further, the new product line includes a smartphone application that allows users to remotely control the appliances. Tasked with conducting a risk assessment of this product line before mass production, the general counsel wants to identify potential issues relating to data created and stored by these smart products.

The Internet of Things

Over the last few years, the use of connected devices has become widespread among consumers and businesses. From thermostats to cars, countless objects now can collect, store and transmit data. The vast network of these connected objects is often called the "Internet of Things" (IoT). IoT devices include smart home technology allowing consumers to control locks, alarm systems, lights and thermostats through their mobile phones; wearable devices monitoring health and fitness; smart cars that offer driver-assist features; and more. IoT technology also is increasingly being used by businesses. Smart manufacturing uses IoT to track assets, monitor inventory and automate factories. Health care providers use IoT technology to track pharmaceuticals, monitor patients' health and send information to doctors. And utilities use smart grid technology to gather data regarding power use and outages.

While this ability to send and receive data provides powerful tools to improve consumer experience and gather information about consumer behavior, IoT presents several information governance and discovery challenges concerning data privacy, information security, and data preservation and extraction.

Data Privacy

The data collected by IoT devices may be subject to privacy regulations and can raise other issues relating to consumers' expectations that certain information will remain confidential. Some voice-controlled IoT devices, such as smart televisions or smart speakers, can (advertently or inadvertently) record conversations users expect to be private. Similarly, connected devices with cameras may record video or capture images without consumer knowledge. Many IoT devices collect, store and transmit sensitive consumer information such as geolocation information, payment details and health data, all of which may implicate state and federal privacy laws. Depending on where the servers storing such data reside, foreign data privacy laws also could

apply.

To ensure compliance with data privacy laws, it is important that companies pay particular attention to the nature of the data being gathered by the device and where the data are being stored. To minimize the risks associated with the inadvertent disclosure of private information, best practices include establishing consent, use and disclosure policies regarding the collection, storage and use of data (including the use of just-in-time notices for the collection of more sensitive information) and minimizing the collection and use of personally identifiable information.

Information Security

IoT devices also present data security concerns. Hackers may target an IoT device to obtain information stored on or communicated by the device. Even more problematic, hackers may attempt to gain control of the device itself either to manipulate it or use it as backdoor into company servers, which puts the enterprise at risk of a large-scale data breach.

To guard against such attacks, companies should consider implementing security safeguards and practices, including engaging an IT security vendor to test the IoT devices and related network to identify potential vulnerabilities. Further, data collected or transmitted by an IoT device and data stored on company servers is substantially more secure if it is encrypted while at rest. If the company is using a third-party storage provider, that provider's security policies and procedures should be fully vetted. The company should also test its software update processes to ensure that security solutions can be delivered in an effective and efficient manner.

Discovery of IoT Devices

Just like traditional forms of electronically stored information ("ESI"), potentially relevant information from an IoT device will be discoverable in a litigation. But the discovery of ESI on IoT devices presents some unique challenges, which include the relationship of the data owner to the litigation, producing the data in a usable format, separating relevant information from the massive amounts of data collected by IoT devices and maintaining consumer confidentiality.

Data collected by an IoT device may reside on the device only temporarily, if at all, before being transferred to a remote server. Due to the cost savings of outsourcing data-hosting services, IoT device data is often stored on third-party servers. While the data may technically be in the possession and custody of the service provider, under most circumstances the device manufacturer maintains control over the data for purposes of triggering a party's preservation obligations under the Federal Rules of Civil Procedure. As part of a comprehensive information governance program, companies contemplating the use of a third-party data storage provider should evaluate the service provider's ability to comply with company data retention policies, including the preservation of data, and to retrieve and deliver company data when necessary.

Conclusion

In addition to their unique benefits, IoT devices present unique information governance and discovery challenges. Companies should consider the potential privacy implications of information gathered by IoT devices and implement data security procedures to prevent the inadvertent disclosure of data. Should litigation arise, data retention policies that ensure proper preservation of information and allow the sorting and production of data will help facilitate the discovery process.

For inquiries related to this Tip of the Month, please contact Lilya Mitelman at lmitelman@mayerbrown.com and Michael Battaglia at mbattaglia@mayerbrown.com

To learn more about Mayer Brown's Electronic Discovery & Information Governance practice, contact Michael E. Lackey at mlackey@mayerbrown.com, Eric Evans at eevans@mayerbrown.com, Ethan Hastert at ehastert@mayerbrown.com, or Edmund Sautter at esautter@mayerbrown.com.

Please visit us at www.mayerbrown.com.