eDISCOVERY BEST PRACTICES:

HOW THE INTERNET OF THINGS CREATES NEW CHALLENGES IN eDISCOVERY

Because technology continually evolves, legal professionals need to understand the latest developments concerning electronically stored information (ESI) and how it affects the legal discovery process. The latter has not changed as significantly as the practices to preserve, collect and produce ESI. There are new twists. One relates to the Internet of things (IoT), a phrase that describes devices that have built-in Internet connectivity and the capability to link to other Internet-connected tools. IoT smart devices include Amazon Alexa, smart watches, fitness trackers, certain household appliances and smart home hubs (hardware or software that connects devices on a home automation network and controls communications among them).

Surveys have shown that there are currently over six billion such devices in use worldwide. Methods for managing and storing the data associated with these devices is diverse and differs from more traditional Internet-connected devices such as laptops, desktop computers, smartphones and tablets. In fact, many IoT devices have limited capability to save the data they generate. Additionally, users may not be aware that because some of these devices lack security applications, the data they create may be regularly deleted or overwritten. Another important element to consider is that some devices, such as smartwatches and smart home devices send their data to a storage server at their company's location. Depending on the company's data retention policies, this data could be the target of legal discovery requests.

CHANGING HOW WE THINK ABOUT DATA

The evolving world of technology is not only driving the explosion of smart devices, it is challenging our thinking about what data is and where it is stored. Previously, data was stored on a local device that had to be physically connected to another device in order to share information. Today's wireless world allows us to link devices without a physical connection.

Beyond that, the IoT utilizes cloud computing that enables devices, networks and virtual storage environments to seamlessly share and automatically back up data. This allows for easily accessing information that is essential to our daily personal and work-related activities.

Until now, eDiscovery demands for electronically stored information (ESI) typically have been limited to document servers, laptops, desktops, email and Microsoft Office data. For eDiscovery purposes, these types of data have defined characteristics as well as easily attainable metadata and text. The eDiscovery process becomes much more difficult when we consider IoT devices.

The two primary areas of concern related to IoT devices and eDiscovery are who owns the data, and how do we retrieve/review the data. The "who" part of this question is still being defined. Rule 26(a) of the Federal Rules of Civil Procedure allows for the discovery of ESI that is in the responding party's "possession, custody or control." Rule 34(a) and Rule 45(a) obligate the responding party to produce ESI that is in their "possession, custody or control."

However, the rules don't necessarily define what is meant by "possession, custody or control." When it comes to a smart device that stores the data on its company's server or in the cloud, locating and collecting data for that particular device can be problematic. If the discovery demand involves participation of a third party that hosts the data, all the "possession, custody or control" issues that you have in traditional discovery will play a factor. At this point there isn't much case law regarding smart devices and who has "ownership" of the data.

WHO OWNS THE DATA?

With email, a user's identity is easily determined. A smart device user's identity may be more difficult to determine than traditional eDiscovery data. Scenarios in which smart devices are shared among multiple people, or possibly lost or stolen, are a factor when determining who has ownership of these devices and their data. Additionally, if you have a smart device in your home such as an Amazon Alexa, and multiple people use voice commands to control that device, a question arises as to who actually "owns" the data. These ownership questions are being considered by legal professionals and governments and there will hopefully be more case law regarding this subject in the coming months.

The small print in contracts, which is often overlooked, speaks to privacy issues about the data that is maintained by a service provider. Amazon's Alexa, for example, offers a series of notices and requires an acceptance of their terms of service. This includes a statement that data is shared with the parent company. "We share user data with our parent corporation, Amazon.com, Inc., and the subsidiaries it controls, and we may share personally identifiable information with third parties only as described ..." This alone can have important implications. Data is shared within the organization that manages the Alexa, but also with a much larger company that can mine the data for its own business purposes. This is not uncommon, and it is becoming a standard business operating procedure because service providers can prosper by sharing and selling data. While these gains lead to innovation, sharing data also creates risks.

THE KEY CHALLENGE

From a discovery perspective, let's assume we know where potentially relevant data is stored and who "owns" it. The key challenge is how do we collect the data and provide it in a

format that is understandable and reviewable. Since there is no standard data format or structure with IoT devices similar to what we have with email and traditional ESI, it makes collecting and reviewing the data exponentially more difficult.

More likely than not, the data is being stored in a structured data format in a database. Structured data has always been a thorn in the side of eDiscovery professionals. The tools most eDiscovery professionals use to process and host traditional ESI are not capable of handling structured data in proprietary formats from smart devices. The industry is working hard to develop new technologies designed to better handle the proliferation of smart device data. Certainly analytics and machine learning tools will play an important role in this respect.

RECOMMENDATIONS

Regardless of the many questions about identifying who owns data and how to collect it, smart devices are here to stay and will increasingly be targeted in litigation and discovery requests. Below are some recommendations to prepare for such requests in the future.

- **Identify cloud computing solutions used by your organization** and then review the security policies you have in place related to those solutions.
- **Determine cloud computing solutions where data is hosted** outside of your organization and review the provider(s) policy for handling third-party subpoenas for your data.
- **Inquire and negotiate terms** for responding to third-party subpoenas and government demands.
- **For corporations, identify a person in your organization** to research and identify potential sources of data from smart devices and determine how the devices fit into your litigation response plan.
- **"Take a walk with the data"** in terms of identifying how specific types of data can be put under a legal hold as well as collected, reviewed and produced.
- **Monitor case law updates** regarding litigation involving smart devices.
- **Identify eDiscovery service providers** that you might consider engaging—companies that are leading the way in developing tools to handle case-relevant ESI.

About Canon Discovery Services

Canon Discovery Services has a skilled, dedicated team of discovery professionals with a proven track record in solving complex discovery matters. Backed by over twenty years of experience, we help law firms and corporate legal departments develop practical, defensible eDiscovery response plans to support successful outcomes. Our services range from ESI processing, culling and analysis, document review, hosting and production to implementing information governance and readiness response programs. Canon Discovery Services is a part of Canon Business Process Services, a subsidiary of Canon U.S.A. Visit us at cbps.canon.com/managed-services/discovery-services.

[1] "Alexa Internet Privacy Notice." Last Updated: May 23, 2018, https://www.alexa.com/help/privacy