IoT Data Collection Raises Legal, eDiscovery Questions

by **Philip Favro** | May 21, 2015 2:48 pm | 0 Comments

Philip Favro, Senior Discovery Counsel, Recommind, Inc.

One of the most anticipated technological trends beginning to confront the business world is the Internet of Things (IoT). The IoT has been in the news for a few years, but for companies, 2014 marked the IoT's emergence as a hot topic. This is due in large part to the increasing number of interconnected devices, applications, technologies, and other innovations that are flooding workplaces, businesses, and even homes.

Given the increasing ubiquity of the IoT, its privacy and security risks, and the potential significance that IoT data could hold in legal matters, organizations should begin making preparations so they are ready when a tidal wave of IoT-related issues arrives.

Two of the more prominent IoT hazards that should be apparent to enterprises are data privacy and information security. These issues come into play when (1) IoT devices inadvertently or intentionally gather personally identifiable information (PII) belonging to consumers or employees; and (2) that PII is then transmitted, processed, and stored by entities tasked with owning and/or operating the device.

Either of the above scenarios could land a company in treacherous legal waters. Sweeping up PII could violate international or perhaps even domestic data protection laws that proscribe the collection of PII, particularly without the data subject's consent. In addition, transmission or storage methods that lack appropriate security may leave PII vulnerable to hacks or other unauthorized interceptions.

Recent problems involving Samsung's smart TVs are particularly instructive on the risky interplay between the IoT, data privacy, and information security. Earlier this year, Samsung acknowledged that its smart TVs could eavesdrop and record viewers' voice commands. Buried in the boilerplate of its privacy policy, Samsung had disclosed that a viewer's "spoken words" in the presence of the TV – no matter how personal – apparently "will be among the data captured and transmitted to a third party through your use of Voice Recognition."

After many media outlets reported on the issue, Samsung revised that provision to clarify and soften its impact.

But that did not end the IoT problems with Samsung's smart TVs. It was subsequently revealed that viewers' voice commands are transmitted to third parties through unencrypted transmissions, making it possible for "a man-in-the-middle in the network to eavesdrop on the data and tamper with it."

Making eDiscovery Waves

Beyond IoT issues like data privacy and information security, there are eDiscovery dangers lurking beneath the surface of companies' information governance programs. These

dangers, which are particularly acute in the context of litigation holds and data preservation, are becoming better known through industry education efforts. For example, a highly publicized session from the 2014 Georgetown Law Advanced E-Discovery Institute brought much-needed attention to the issues. During that session, speakers representing various constituencies observed that the IoT could raise any number of preservation and production challenges in the discovery phase of civil litigation. Ignatius Grande from the law firm of Hughes, Hubbard & Reed explained that the IoT was not designed to accommodate eDiscovery demands:
"Many products in the IoT sphere are not created with litigation hold, preservation, and collection in mind," he said. "In terms of liability . . . companies will most likely be responsible to preserve data produced by the capabilities of their products and services in the event of a litigation hold."

Thus, unless appropriate measures are adopted to ensure that IoT data is preserved for litigation or regulatory matters, relevant IoT materials could be lost, setting the stage for expensive and time-consuming satellite litigation.

Smooth Sailing Ahead?
As the foregoing illustrates, organizations need to have an actionable plan to prepare for the data privacy, information security, and eDiscovery implications of the IoT. As an initial phase in this preparation, companies should determine the extent to which the IoT affects or will affect their consumers and employees. Understanding the range of potential IoT issues will provide clarity on the next steps that should be taken.

One of those steps likely will involve the development of an information governance strategy that accounts for the IoT. Such a strategy should include a plan for identifying information that must be kept for business or legal purposes while isolating other data (particularly PII) for eventual deletion. It also should encompass steps to ensure compliance with the privacy expectations of domestic and international data protection authorities. Enterprises also will need to ensure that their litigation readiness programs are updated to include a process for preserving and producing relevant IoT data.

Taking a proactive approach that addresses these issues will help companies avoid many of the treacherous problems associated with the IoT. While it may not lead to smooth sailing all of the time, it will establish a process that can enable the successful disposition of IoT issues.

Philip Favro brings over 14 years of expertise to his position as Senior Discovery Counsel for Recommind, Inc. Phil is an industry thought leader, a global enterprise consultant, and a legal scholar on issues such as eDiscovery, information governance, and data protection.