EVOLVING TECHNOLOGY AND THE PRIVACY EFFECT

February 28, 2019

By Matthew McCabe, Senior Vice President and Assistant Counsel, Cyber Policy

This article was originally written for Advisen Front Page News

Risk managers know that companies create data privacy risk by collecting, storing, and processing data. But a full assessment of data privacy risk requires another important step. Companies must look not only at the type of data being collected, but also how the rapid evolution of technology can make collected data increasingly sensitive to individual privacy concerns.

This relationship between evolving technology and its effect on data privacy was examined in a recent Supreme Court case, *Carpenter v. United States*. In *Carpenter*, the Court considered whether police needed to obtain a warrant for collecting cell site location information (CSLI), which is generated whenever a cell phone comes within range of a tower. CSLI can reveal the time, duration and location of the call.

In *Carpenter*, police used CSLI to match the location of several suspects with times and places where numerous robberies occurred. In obtaining the data, the police never sought a court-approved warrant. Instead, they relied on an administrative process under federal law and requested the records from the phone carrier.

The police request had strong precedent. Years ago, police often asked phone companies to place a "pen register" on a suspect's phone line that would record the called number, when the calls were made, and how long the call lasted. Individuals had no expectation of privacy in this data because the suspects voluntarily gave that information to a third party — the phone company. Under this "third-party doctrine," courts found that individuals had waived any expectation of privacy in that data simply by purchasing phone services.

This "third-party doctrine" potentially applies to lots of data, such as bank, employment, and transaction records. Naturally, the loss of privacy through transactions did not sit well with many. As a result, federal and state governments passed laws to protect data, like state data breach laws, the Health Insurance Portability and Accountability Act, the Gramm-Leach-Bliley Act and more. *Carpenter*, however, disagreed that the third-party doctrine deprives robbery suspect of a privacy interest in that data. Instead, the court found that CSLI is highly sensitive due to its "deeply revealing nature . . . its depth, breadth, and comprehensive reach, and the inescapable and automatic nature of its collection."

Importantly, the *Carpenter* decision applies in the narrow context of criminal searches and relies on specific legal precedents. However, risk managers should take to heart some practical implications:

- Data no longer stands alone. The digitization of all types of data, combined with widespread collection and a massive increase of computing power, provides companies with a powerful ability to learn about individuals. Even where data may not appear particularly sensitive, our ability to cross-reference data and store it indefinitely might provide more revelations than originally assumed. Refining this ability means a heightened risk of data privacy.

- Companies must monitor how widely adopted a technology has become. Simply put, what was voluntary yesterday may not be so now. *Carpenter* recognized that cell phone use is ubiquitous in today's world. As a result, cell phone users should not be viewed as "voluntarily" waiving rights to privacy by using such a pervasive technology. The more commonly used a technology becomes, the more likely the use of that technology could be considered "non-voluntary," and the more likely data shared through that technology will be protected.

- Companies' protection of privacy should consider not only today's processing of data, but also how technology will foreseeably advance. Current CSLI technology might put you within a mile of a user's location, but *Carpenter* recognized that "soon and inevitably," CSLI technology is going to improve and the privacy considerations will be even greater. When evaluating data privacy, businesses must predict how rapidly their technology will develop and whether that evolution will provide a greater ability to identify traits of specific individuals.

Today, our everyday activities are being monitored, recorded, and analyzed. Increasingly, drivers rely on GPS technology for directions. Stadium events routinely use facial scanning to identify potential threats. Recently, a Chinese company announced the development of "gait recognition" technology, which identifies individuals by how they walk with a 94% accuracy rate. As these technologies become more sophisticated and are more widely deployed, the companies using the data behind them must account for how privacy is affected.

While this refinement of technology increases data privacy risk, regulatory obligations for data privacy requirements have also intensified. Europe's General Data Protection Regulation (GDPR) led the movement with new mandates, individual rights, and the potential of mammoth fines. Soon, several more nations mimicked GDPR requirements. Recent large fines issued under the GDPR have served to remind industry of the potential impact of violating these new data privacy laws.

Notably, one measure introduced by the GDPR was a requirement for undertaking a privacy impact assessment. Companies undergoing this assessment, or any similar privacy impact analysis, should evaluate how technology is changing in a manner that might more clearly identify an individual or information about that person.

Those companies not scrutinizing the effect of technology on privacy might be missing an important step in the process. The evolution of your technology could bring data privacy regulators to your door faster than you think.