Drinker Biddle

Client Alert

September 7, 2016

Reasonable Expectations of (Data) Privacy in the Digital World?

By Kenneth K. Dort, Katherine E. Armstrong and Jennifer T. Criss, Ph. D.

Relying on the third party doctrine, the U. S. Court of Appeals for the Seventh Circuit issued its ruling in *United States v. Caira*, a decision that directly addresses the expectation of privacy in one's home but that indirectly impacts the expectation of data privacy in the digital world. The ruling was issued on Aug. 17, 2016.

Background

In *Caira*, the Drug Enforcement Administration ("DEA") monitored an overseas website that supplied sassafras oil, an ingredient used in creating the drug ecstasy. After learning that numerous e-mails were sent in 2008 to the website's e-mail address from a particular Hotmail e-mail address, the DEA served an administrative subpoena on Microsoft, the owner of Hotmail. The subpoena asked for all subscriber information related to the specific Hotmail address, including subscriber name and address and the "account login histories (IP Login history)" of the account. Microsoft complied with the subpoena and furnished information about the account, including Internet Protocol, or IP, addresses from which the Hotmail account was accessed.

The DEA determined that one frequently-used IP address linked to the Hotmail account and identified by Microsoft was owned by an unrelated internet service provider, which the DEA then served with an administrative subpoena for information about that address. In response, the ISP provided the DEA with the name and physical address of the user associated with the IP address. The DEA ultimately charged the user's husband, Frank Caira, with possessing and conspiring to manufacture illegal drugs. He was ultimately convicted on those charges in the U. S. District Court for the Northern District of Illinois, and he appealed.

Reasonable Expectation of Privacy

At issue in *Caira* was whether the defendant had a reasonable expectation of privacy in his IP address, which was associated with his physical home address. The Fourth Amendment to the U.S. Constitution provides that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated."

The Supreme Court has held that a search violates the Fourth Amendment when "the government violates an expectation of privacy that society recognizes as reasonable." *Kyllo v. United States*, 533 U.S. 27, 33 (2001). Caira argued that, because (1) the DEA discovered the IP address associated with his home, (2) the DEA knew the address would likely be his home since that is a location from which individuals frequently check their e-mail account, and (3) the home is given special protection under the Fourth Amendment as a place where a reasonable expectation of privacy exists, the DEA's "search" was unreasonable. Therefore, Caira reasoned, any information uncovered by that search should be suppressed. The Seventh Circuit disagreed with Caira. It affirmed the decision of the district court to deny Caira's motion to suppress the use of the data against him.

The Seventh Circuit stated that Caira had voluntarily shared his IP address with a third party, namely Microsoft, when accessing his Hotmail account from his home computer. The court likened the transmission of such data from Caira's ISP-owned IP address to Microsoft's e-mail servers to the conveyance of telephone numbers to a telephone company when placed calls are routed through the telephone company's switching equipment. Such disclosure, the court stated, was voluntarily given under what is known as the "third party doctrine." Under this doctrine, "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties . . . even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed." *United States v. Miller*, 425 U.S. 435, 442-44 (1976). Consequently, the Seventh Circuit held that Caira had no reasonable expectation of privacy in his IP address and affirmed the denial of his motion to suppress the data collected by the DEA.

Implications for Data Privacy

Under *Caira*, the third party doctrine continues to apply to the expectation of privacy with regard to personal information: if such data is voluntarily disclosed in any way, an individual cannot maintain any reasonable expectation of privacy as to that data.

In the analog world, what constitutes a "voluntary" disclosure is relatively straightforward. But how can one define a "voluntary" disclosure in the digital universe, where such disclosures may be happening under the surface and without the explicit knowledge of or any affirmative action by the owner of that data? Could Caira really have "voluntarily" disclosed his IP address to Microsoft, a process that happened instantaneously, automatically, and without any direct act on his part? Did he even know that such information existed, let alone was being shared -- a digital footprint of Caira's path through cyberspace?

Despite the Seventh Circuit's ruling in *Caira*, there are signs that changes may be coming to the applicability of the third party doctrine to the digital landscape. In the recent Supreme Court decision in *United States v. Jones*, 132 S. Ct. 945 (2012), the concurring opinions of Justices Sotomayor and Alito, joined by three other justices, critiqued the third party doctrine, expressing views that 21st century technological developments have dramatically increased the amount and precision of data the government can collect about individuals with relatively little effort.

The Supreme Court has upheld the third party doctrine, including in certain digital contexts, and the *Caira* decision follows Supreme Court precedent. But five sitting Supreme Court justices (Alito, Sotomayor, Ginsburg, Breyer and Kagan) recognize that the third party doctrine may not be one-size-fits-all and equally applicable to the analog and digital worlds, where explicit actions are replaced by implicit and abstract consent to the transfer of data. As a result of this growing dichotomy, the third party doctrine may one day be modified to adapt better to the reality of 21st century technology.

What's an Internet User to Do?

On the heels of *Caira*, anyone using the Internet to transmit information – whether by viewing a website, downloading a song, or merely checking one's e-mail – should be aware that, under current law, there should be no reasonable expectation that such information will remain private. An individual need not realize that his actions create a digital paper trail or that his data is being shared with third parties without any explicit actions on his part; the third party doctrine remains valid. As the reality of applying the third party doctrine to evolving technology continues to be evaluated, however, changes to the law may be coming, perhaps sooner than we think.

And it could be worse. Frank Caira is currently serving a life sentence for a conviction in a separate case – in an attempt to avoid conviction on the drug charges discussed above, he also tried to have the prosecutor and DEA agent murdered. Perhaps granting implicit consent to transmit one's digital data to third parties through cyberspace is not so bad after all.

Information Privacy, Security and Governance Team

Primary Contacts

Kenneth K. Dort
Partner
Chicago
(312) 569-1458
Kenneth.Dort@dbr.com

Katherine E. Armstrong
Counsel
Washington
(202) 230-5674
Katherine.Armstrong@dbr.com

Jennifer T. Criss, Ph. D.
Associate
Washington
(202) 230-5648
Jennifer.Criss@dbr.com

Drinker Biddle®

www.drinkerbiddle.com

CALIFORNIA | DELAWARE | ILLINOIS | NEW JERSEY | NEW YORK | PENNSYLVANIA | WASHINGTON DC | LONDON