Professor Tokson Shines a New Light on Privacy

His article, selected for a law schools conference and a law review, explores how much people know about their right to be let alone

Professor Matthew Tokson has absolutely no expectation of privacy for an article he wrote about privacy.

The Southeastern Association of Law Schools has asked him to discuss it at its annual meeting in August, and it will be published this year in the *Northwestern University Law Review*.

The article, entitled "Knowledge and Fourth Amendment Privacy," looks at how courts rely on societal knowledge to determine reasonable expectations of privacy throughout society. Many of those expectations have had decades to develop: Louis Brandeis wrote in 1890—twenty-six years before he was appointed to the Supreme Court of the United States—of a right to be let alone, and Justice William O. Douglas identified in 1965 a right to privacy in the penumbra of the U.S. Constitution.

Professor Matthew Tokson

But when expectations move forward to a digital age, some courts might measure what people could be presumed to know through societal knowledge in small bits and bytes of knowledge. Although most people might be expected to know that a 5G cell phone will be faster than a 4G phone, there might be little else courts would uniformly presume people to know when they turn on phones or computers and later find that calling locations had been tracked or email addresses had been captured.

What courts often conclude about what people commonly know about privacy when they cross into the digital frontier is often incorrect, Professor Tokson determined in his article. "It finds that assessing societal knowledge about privacy is inherently difficult, that courts often err in determining societal knowledge, and that relying on knowledge to determine the scope of the Fourth Amendment would be problematic even if courts could assess it perfectly," he says.

Based on excerpts from Professor Tokson's article, here are two things cell phone and computer users might be presumed to know or not to know about expectations of privacy in a digital world:

The location where a cell phone call originates may or may not be a private matter, depending on the state from which the call is made. On this, Professor Tokson cites splits among federal courts of appeals:

The Third Circuit [Delaware, New Jersey, and Pennsylvania] held that a cell phone user had not waived his privacy in his cell phone location data, because "it is unlikely that cell phone customers are aware that their cell phone providers collect and store historical location information."

The court's reasoning was that "[w]hen a cell phone user makes a call, the only information that is voluntarily and knowingly conveyed to the phone company is the number that is dialed, and there is no indication to the user that making that call will also locate the caller."

The Fourth Circuit [Maryland, North Carolina, South Carolina, Virginia, and West Virginia] recently agreed, finding Fourth Amendment protection for cell phone location data because "[w]e have no reason to suppose that users generally know what cell sites transmit their communications or where those cell sites are located."

The Fifth Circuit [Louisiana, Mississippi, and Texas] reached the opposite conclusion. It ruled that "users know that they convey information about their location to their service providers when they make a call and … they voluntarily continue to make such calls," thereby waiving their privacy. The court reasoned that cell phone companies' terms of service and privacy policies "inform subscribers that the providers not only use [cell phone] information, but collect it."

The Eleventh Circuit [Alabama, Florida, and Georgia] has also denied Fourth Amendment protection for cell phone location data, determining that cell phone users "know… that cell phone companies make records of [their] cell-tower usage." The court found that there were sufficient "publicly available facts" regarding cell phone location data that cell phone users could have no reasonable expectation of privacy in their location data.

Societal knowledge about old technology might apply by analogy to new technology. On this, Professor Tokson wrote:

For example, in United States v. Forrester [(2007)], the Ninth Circuit answered the novel question of whether the Fourth Amendment protects email to/from addresses and the IP addresses of the websites that a user visits by drawing a parallel to the [U.S. Supreme] Court's assessment of collective knowledge [in *Smith v. Maryland* (1979) about the use of a pen register installed on phone company property to record dialed telephone numbers].

The Ninth Circuit noted that "*Smith* based its holding that telephone users have no expectation of privacy in the numbers they dial on the users' imputed knowledge that their calls are completed through telephone company switching equipment." It then held that website and email to/from addresses are not protected by the Fourth Amendment because of the knowledge of Internet users.

"Analogously, e-mail and Internet users have no expectation of privacy in the to/from addresses of their messages or the IP addresses of the websites they visit because they should know that this information is provided to and used by Internet service providers for the specific purpose of directing the routing of information."

Other courts have reached the opposite conclusion regarding website IP addresses, based on a different analysis of users' knowledge about the Internet [with the New Jersey Supreme Court determining in *State v. Reid* (2008)]:

"[W]hen users surf the Web from the privacy of their homes, they have reason to expect that their actions are confidential. Many are unaware that a numerical IP address can be captured by the websites they visit. More sophisticated users understand that that unique string of numbers, standing alone, reveals little, if anything, to the outside world."

> "Assessing societal knowledge about privacy is inherently difficult, courts often err in determining societal knowledge, [and] relying on knowledge to determine the scope of the Fourth Amendment would be problematic even if courts could assess it perfectly."

Many users' lack of understanding of how websites operate, coupled with other users' awareness of the technical specifics of IP addresses, provided the basis for a reasonable expectation of privacy.

In the first set of cases to address whether government collection of the contents of emails is covered by the Fourth Amendment, the Sixth Circuit [in *Warshak v. United States* (2007)] held that the question depends on the knowledge of email users. The judges inferred customers' knowledge based on the user agreements that their email service providers promulgate. Thus, "where a user agreement explicitly provides that e-mails and other files will be monitored or audited …, the user's knowledge of this fact may well extinguish his reasonable expectation of privacy."

The Sixth Circuit noted that the Fourth Amendment inquiry "may well shift over time" and would "assuredly shift from internet-service agreement to internet-service agreement." It ultimately concluded that the defendant had a reasonable expectation of privacy in his emails because his ISP user agreement did not inform him that the ISP would "'audit, inspect, and monitor' its subscriber's emails."