New Jersey Law Journal
STATEWIDE LEGAL AUTHORITY SINCE 1878

Is N.J. a Bellwether in Privacy Debate?

August 15, 2013

By Nicholas W. Allard

The New Jersey Supreme Court's unanimous ruling in July that police must obtain warrants to access information on a crime suspect's cellphone location puts the balance between protecting citizens' safety and their privacy front and center.

New Jersey is the first state to go that far in favor of privacy. Chief Justice Stuart Rabner wrote in *State v. Earls*, A-53-11, "No one buys a cell phone to share detailed information about their whereabouts with the police."

Retired Chief Justice James Zazzali, Rabner's predecessor, said, "Our Supreme Court, once again, has demonstrated its vigilance in protecting the privacy rights of our citizens when Big Brother intrudes or overreaches."

The Rabner court also ruled that even in child sex-abuse investigations, police must get approval from a high-ranking prosecutor to conduct wiretaps.

The far-reaching implications of this ruling will be a reference point for other states. Technology is pushing boundaries with tools that can now rapidly and continuously collect massive amounts of data — right down to when you made your last phone call — and analyze it quickly.

The phenomenon known as big data is making privacy rights the biggest civil rights issue of our time.

Why? Because there are two sides to the big data story: the good and the invasive. In between are 1,000 shades of gray.

You decide where the following examples fall on that spectrum:

• The chief of the National Security Agency (NSA), General Keith Alexander, testified that the U.S. government's domestic intelligence programs have "disrupted" more than 50 terrorist plots against the U.S. and its allies.

• U.S. federal prosecutors just charged four Russian nationals and a Ukrainian for stealing 160 million credit card numbers. Law enforcement officials monitored the hackers' communications, including personal instant messages.

• Late last month, the FBI arrested more than 150 suspected pimps and rescued more than 100 children in a nationwide child sex trafficking sting. The FBI routinely worked with agencies around the country to gather and analyze information about suspected traffickers.

Even though mass and targeted surveillance can thwart terrorist or criminal activities, this kind of information gathering by government and law enforcement is under a microscope. Case in point is Edward Snowden, the NSA contractor who leaked top-secret information about U.S. and British mass surveillance programs to a reporter.

Beyond data gathered by government agencies, there is the data gathered by commercial and other enterprises when users visit websites.

The Wall Street Journal recently reported experts' estimates that an active Google user can generate hundreds or thousands of data events every hour, which Google stores and makes available to advertisers for upwards of $50 billion a year.

Another recent *Wall Street Journal* story examined about 1,000 top websites and found that 75 percent of them now include code that can match people's real identities with their Web-browsing activities.

And the New Jersey Division of Consumer Affairs just reached a $1 million settlement with PulsePoint, an online advertising company that used hidden code to allegedly bypass privacy settings of consumers' web browsers without consent.

New Jersey certainly feels compelled to act, and other states might as well. But a state-by-state approach will result in a patchwork quilt pattern of different laws. Among the 50 states, there are 46 different state laws governing corporate responses when databases are hacked.

In contrast, there is a policy vacuum at the federal level with relatively few laws that protect privacy. Exceptions are laws that protect our financial and medical information and information that our schools gather about our children.

That's because historically, America has been ambivalent, if not conflicted, about privacy. Our ambivalence is about to end. In a digital world, it is virtually impossible to protect your own data privacy. The question is: Will the federal government impose a uniform approach or will states decide?

Despite the shades of gray, one thing is clear: protecting our privacy will require a new generation of lawyers steeped in privacy law and the implications of big data.

This coming demand puts a new responsibility on law schools to ensure that we are prepared to address for the coming explosion of privacy concerns.

It doesn't get much more black and white than that. And right now, New Jersey is leading the way.

Allard is the Joseph Crea dean and professor of law at Brooklyn Law School, where he teaches information privacy law. Before Allard became dean, he was a partner at Patton Boggs.