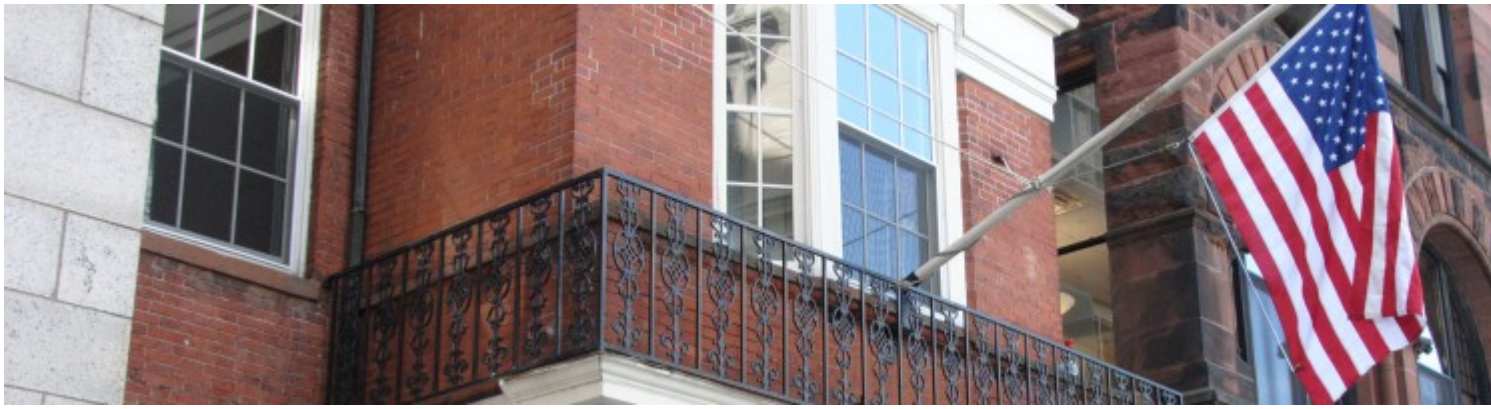
Boston Bar Journal
A Peer Reviewed Publication of the Boston Bar Association



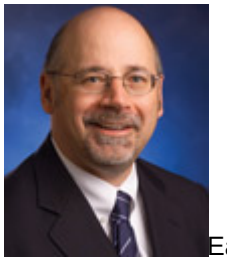
← Oh, the Places You've Been! Preserving Privacy in a Cellular Age
Sealing the Virtual Envelope: Protecting Attorney-Client Privileged Email in Criminal Investigations →

Don't Click This Article!

Posted: September 12, 2012 | **Author:** bbabarjournal | **Filed under:** Fall 2012, Vol 56, #4, Vantage Point | **Tags:** data enrichment, privacy, privacy in digital age |Leave a comment »

By Richard J. Yurko

Vantage Point



Each of us lives in a digital soup where, every day, we leave an online record of our activities. For the convenience of an ATM card, we leave traces of our banking transactions. For the social benefit of "connecting" with acquaintances, our Facebook, Twitter, Linked-In, email, and other accounts record what we look at and digitally touch. For the sake of a few cents off at the store, our loyalty cards compile a rich history of our shopping habits. For the sake of our iPhone, we let Apple know our location virtually every moment of the day. This digital soup not only has practical implications for everyday life, but also potentially changes the landscape of two core legal doctrines, the constitutional right to be secure in our private affairs from government

intrusion and the common law right to be let alone from private actors. These issues recently surfaced within a divided United States Supreme Court.

Thousands of digital data points can be and are being aggregated, cross-referenced, and enriched with still other data, like public records, our credit scores, and political donations. *See, e.g.,*Sullivan, "**Data Snatchers! The Booming Market for Your Online Identity**", PCWorld.com (June 26, 2012); Sengupta, "**Should Personal Data Be Personal**?", New York Times (February 24, 2012). This enriched data is, in many respects, more thorough, more accurate, and more detailed than any file ever compiled by J. Edgar Hoover. It is possible that we can be known better by these data aggregators than by our own friends and kin.

I am annoyed when data aggregations are used to try to sell me a particular product that just happens to be on sale at a store on my walk to work. Individually, I am not much troubled by the use of this data by the company that first collected it, which may track what brand of over-the-counter headache medicine I buy so that it can offer me an appealing coupon. I am much more troubled if the first party that collected the information then sells it to third parties with unknown motivations – - commercial, political or nefarious.

Annoyance and displeasure give away to apprehension when purchased data can be enriched and cross-indexed with other information and then used by powerful corporate interests without my knowledge or anticipation. Moreover, what is to prevent the government from routinely accessing or purchasing such detailed, enriched data aggregations for any purpose? And if the government could buy such data aggregations, what is to stop the government from simply requesting and obtaining the same material from private aggregators, without any subpoena, warrant or judicial oversight?

Indeed, the availability of this detailed information can be used to undermine the underpinnings of essential constitutional safeguards or the common law right to privacy. Although, certainly, the constitutional right to privacy is substantially different from the common law right to be let alone, they share one common foundation. Often, both common law and constitutional principles are grounded on the "reasonable expectations" of the parties and, with respect to privacy, those expectations may be less reasonable if intensely personal data is freely available to anyone who wants to buy it.

That issue was recently raised in **United States v. Jones**, 132 S. Ct. 945 (2012). In Jones, the majority opinion, authored by Justice Scalia and joined by Justices Roberts, Kennedy, Thomas, and Sotomayor, avoided complex issues arising from the warrantless attachment of a GPS tracking device to a suspect's automobile by resorting to the 18th Century common law of trespass. The majority concluded that, because the installation necessarily involved a trespass to the suspect's property right in his vehicle, the resultant search and seizure required a warrant. A four-justice concurrence would have found the search and seizure impermissible without a warrant, on a different ground, because it violated the suspect's "reasonable expectation of privacy," relying on **Katz v.United States**, 389 U.S. 347 (1967). The concurrence, authored by Justice Alito and joined by Justices Ginsberg, Breyer, and Kagan, rejected the majority's resort to trespass law as too narrow a basis for principled application going forward.

By far, however, the most provocative question in Jones was raised by Justice Sotomayer in her lone separate concurrence. Justice Sotomayer joined with the majority but she wrote separately, I believe, to raise a question. She was apparently unwilling to join the four-justice concurrence, applying the "reasonable expectation of privacy" test, because she suggested that our notion of privacy may have to undergo reevaluation in a world in which, with varying degrees of inattention and consciousness, we tolerate third parties collecting a wealth of personal data about us.

Questions about the collection, retention, supplementation, use, misuse, sale, dissemination, and extensive re-use of detailed personal data could be thrashed out in Washington, in fifty state legislatures across the country, or through regulations promulgated elsewhere in the world. Indeed, there are conversations on these subjects at the Federal Trade Commission, in some state legislatures, and in the European Union. There is an outside chance that, just the way child labor laws, worker's rights, consumer rights, and economic justice notions were debated and decided in the state legislatures and then again in Congress, this would happen on questions of privacy in the digital age. The FTC has issued papers in this area and may well act. See Federal Trade Commission,**Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers** (FTC Report, March 2012); see also **Consumer Data Privacy in a Networked World**, The White House, (February 2012) (recommending legislative and regulatory action).

But I am not optimistic that these issues will be decided quickly or at all by legislative or regulatory means. The corporations that collect, dissect, enrich, and/or package your personal data for resale are some of the most powerful companies in the world. Rashid, "**Google, Microsoft Survival Conflicts With Internet Data Privacy**," eWeek.com, February 7, 2012. Quite possibly, in their own enlightened self-interest, they may block legislative or regulatory action. Moreover, one can question, in this rapidly evolving digital world, whether any law or regulation can sufficiently address the myriad ways in which data can be collected, aggregated and re-used. Any regulation on, say, the use of "cookies," could be outmoded even before being promulgated or implemented. Courts, by contrast, exist to decide questions that arise in disputes between contending parties and decisions on principles in those cases can extend across technological platforms. That is how the common law developed and, to some extent, how constitutional law has progressed as well.

Well over a century ago, Louis Brandeis and Samuel Warren wrote their seminal piece articulating a right to privacy in the Harvard Law Review. At that time, the danger seemed to come from yellow journalists writing about and photographing private persons to satisfy what was characterized as a public lust for gossip. Brandeis and Warren wove together hitherto unconnected strands of cases to fashion an argument for a common law right to privacy. By giving such a name to the "right to be let alone," they gave lawyers and judges a means to articulate the right to control the intimate details of one's own life. The premise of Warren and Brandeis, however, was that privacy was like the water from a spigot with the individual controlling the spigot. Samuel Warren & Louis Brandeis, **The Right to Privacy**, 4 Harv. L. Rev. 193, 198 (1890). They said, "The common law secures to each individual the right of determining, ordinarily, to what extent his thoughts, sentiments, and emotions shall be communicated to others."

In the last two decades, rapid technological change and remarkable inattention by the public at large have seemed to cede control of that spigot to Facebook, Apple, and hundreds of other less-well-known companies. If these corporations now control the spigots of our personal details shared online, can the government hand be far away? If the government is buying and using the data, will we ever know? If the government is buying the data, should there be some control on that? Conversely, if we see the greater danger as coming from misuse by private parties of digital data aggregations, is government actually the solution, not the problem, by regulating how and when such information can be collected and shared?

Whether in the role of common law jurists or constitutional arbiters, it may rest with judges to take the first stab at re-examining the right to privacy, or the "reasonable expectation of privacy," in a digital world. The right to be let alone from government interference has, obviously, a constitutional dimension. The right to be let alone from private interference, as a common law principle, applies to private as well as governmental actors.

In conversations in judges' chambers across the country, the judicial branch may be asked by litigants to return some measure of control of the spigot of private data to the individual. It should be a lively discussion between judge and law clerk. Judges, generally a generation older than their clerks, will remember a time when the public reacted with shock to governmental dossiers and enemies' lists. Law clerks, some of whom may have grown up in the digital soup and the stunning trade-off between privacy and convenience, may have an entirely different view. Together, they may be able to fashion a new understanding of privacy where incidental disclosure to a third-party providers of services simply through the use of everyday electronic gadgets does not eliminate the broader right to be "let alone." That, at least, is my hope, so that we can move towards the new understanding of privacy rights in a digital era of pervasive commercial tracking.

Rich Yurko *is the founder of the Boston business litigation boutique, Yurko, Salvesen & Remz, P.C., which publishes a weekly* ***Boston business litigation update****.*