DAVID P. MIRANDA

Balancing Act

We have met the enemy and he is us.
– Pogo

We are embroiled in a debate over privacy and whether it has limits, which at times takes on the tone of Patrick Henry's statement, "Give me liberty or give me death." Fortunately, we have more than just those two options. In reality, today's less dramatic data-driven rallying cry is closer to something like "give me privacy or at least give me something slightly entertaining." We compromise privacy to give a few dozen of our close friends and followers full access to our most private and personal information – everything from where we are, to who we're with, to what we eat and think and do. There are no regulations against our "sheep-like" uploading and distribution of personal data, but we draw the line when our government says it needs minimal access to help protect us.

Our inability as a nation to reasonably and intelligently address the issue of data privacy is exemplified by the U.S. Justice Department's need to use an 18th century law to force Apple to override privacy protections on a terrorist's iPhone. In seeking its court order, the Justice Department relied on the 1789 statute known as the All Writs Act, which essentially says that courts can compel third parties to comply with and take action to carry out orders in certain circumstances. Clearly, such an order would have met with much less resistance from Apple and the court of public opinion even just a few years ago, before Edward Snowden brought to light the government's rampant collection, storage and review of private telephone communications data.

Regardless of whether one considers Snowden a traitor or a hero, his revelations have shined a hard light on the lengths our government will go to to collect and curate data. Who we talked to, and when and what was said, was and is culled from the massive amounts of phone data collected, including communications with an expectation of privacy, such as attorney-client communications.

One's right to privacy, however, is determined by whether there is a reasonable expectation of privacy. There are, for example, levels of company-employee interaction and control when a device is used for company business. There is a spectrum of privacy – from a device issued by an employer for use in company business only to a personally enabled device – where the individual owns the device and creates a space on it for his or her own private personal use.

In the San Bernardino terrorist case, county officials owned the phone, gave consent to have the phone searched and gave Apple permission to do so. Apple, however, views its role through the lens of protecting the personal data of the user, not the wishes of the owner of the device. It appears to many that Apple's stance is more of branding and marketing than of privacy or patriotism. Particularly if the issue of ownership of a device affects the disposition of data, it's a fair question whether an employee-user would have reasonable expectation of privacy.

The San Bernardino case has encouraged discussion of federal legislation to require companies to decrypt data if a court orders it to do so. But there has been some reluctance in Congress. In response to the California and New York legislatures' introduction of bills to require smartphone makers to include a back door for decryption and to levy fines for noncompliance, Congress has introduced the ENCRYPT Act (Ensuring National Constitutional Rights of Your Private Telecommunications). The Act would prevent states from passing their own decryption laws. The Act's sponsor

David P. Miranda can be reached at dmiranda@nysba.org.

noted in an interview with *Newsweek* that it wouldn't be feasible to "make one smartphone for California and New York and another one for Minnesota and Texas." It is unclear, however, whether Congress intends to introduce legislation to formulate a national policy.

The issue goes beyond our nation's borders, and even wise regulation in the United States might not fit neatly in our digital world. The European Union has taken a very strong stand against the sharing of personal data without one's consent. Thus, even inadvertent sharing of personal data of an employee in a European company with people in its U.S. office (such as a multi-national law firm) could be deemed unlawful, and data transmissions could be halted. After complaints in the EU about the privacy of social media users' online messaging, the EU's previous privacy policy was invalidated. The EU's Safe Harbor had allowed U.S. companies to self-certify that company practices ensured an adequate level of protection for personal data. Now, the EU is implementing a more stringent policy with greater safeguards. The new arrangement, the EU-US Privacy Shield, will greatly affect corporate policies and internal structures on how companies handle personal data. Interestingly, our U.S. Congress recently passed the Judicial Redress Act, which allows citizens of designated foreign countries and regional economic organizations to bring civil actions against U.S. agencies that are in breach of data protection policies.

Europe is also at the forefront of a personal "right to be forgotten." An article by Steven Bennett in the January 2016 issue of the *Journal* covered a decision by the EU Court of Justice, which established not only a fundamental right to privacy, but a right to have information expunged and forgotten. The ruling required review of each case before a "delisting" request is granted, and made clear that mere inconvenience is not grounds for delisting. The question of whether such delisting must occur only in the countries where suit is brought, or whether it must be implemented internationally, still has no clear answer.

Yet, it is hard on some level to square all this with the reality of our data-driven world. The question may, in the end, be moot because we consistently and freely give away our personal data for a $5 coupon or a free app. Whether you are making a purchase in person or online, your data is collected. If you use a discount card, your every purchase is recorded, and marketing pitches are tailored ever more specifically to you. Buy something online and nearly every time you go to a shopping site, your screen will also show you the latest deals and trends from the companies that sold you your most recent purchases. Every transaction requires a compromise or a tradeoff. We can't pick and choose who gets our data – the shoe store or the government – unless we go off the grid entirely.

For lawyers, a breach of privacy or compromised client data spells disaster. Maintaining the confidentiality of client communications is one of the mainstays of our rules of ethics and professional conduct. In 2008, recognizing the ever-growing importance and difficulty of protecting client data in an increasingly electronic world, then-NYSBA President Bernice Leber created a Task Force on Privacy. The Task Force issued its report in April 2009 – generations ago in our digital era. But, based in sound scholarship and logic, the report has much to tell us about the world we live in today and doing our due diligence as lawyers. It took a clear-eyed view ("[we] recognize that just in the time this Report was drafted, the law has changed and technology has advanced. . . . Some parts . . . could therefore become dated even before [it] is distributed") and repeatedly urged "the Association to continue to examine the sufficiency of the law and its enforcement . . . and update this Report regularly on an as-needed basis."

The job of the Task Force was "to examine privacy issues impacting lawyers and their clients." Seeing the enormity of its task, the Task Force narrowed its focus to a few key areas of law: intellectual property, criminal law, health law, employment law, business law and civil litigation. Across the board, a major concern was on data collection – via the Internet and WiFi, cell and smartphone, GPS technology, E-Z Passes, ID badges, credit card use, surveillance cameras and scanning devices in public facilities and airports. Each area of law had particular concerns: criminal law, where limitations on the privacy of attorney-client communications were singled out; health law, where issues of the security of electronic health records came up; employment law, addressing issues of employees' after-work activities; business law, particularly in the area of identity theft; and civil litigation, balancing the need for discovery and the need for privacy. The Task Force concluded:

> [T]he law is developing to address the challenges raised by technological advances that have caused the world to be "smaller" and privacy to be more difficult to maintain. As lawyers, our role as advisors is impacted both personally and professionally. . . . [T]he Task Force suggests the Association proceed to the next step of exploring those issues, identifying a collective view, and outlining a plan of reform, where necessary.

Pogo hinted at what the real issue may be: our biggest problem is not our government, or foreign governments, or corporate interests, but our own willingness to give our privacy away. ■