Feb 13 2013

Posted By: Mark F. Foley

Practice Area: Information Technology, Data Privacy and Security

Sun Microsystems' CEO Scott McNealy famously quipped to reporters in 1999: "You have zero privacy anyway. Get over it." *Sun on Privacy: 'Get Over It', WIRED*, Jan. 26, 1999.

At the time, Sun Microsystems was a member of the Online Privacy Alliance, an industry coalition seeking to head off government regulation of online consumer privacy in favor of industry self regulation. Although McNealy was widely criticized for his views at the time, it is fair to say that much of the technology world agreed then, or agrees now with his remark.

Have we gotten over it? Do we reside in a world in which individuals assign so little value to personal privacy that companies who collect, process, analyze, sell, and use personal data are free to do whatever they want?

There are indications that if it ever were true that consumers did not value privacy, their interest in privacy is making a comeback. Where commercial enterprises do not align their practices with consumer expectations and interests, a regulator will step in and propose something unnecessarily broad and commercially damaging, or outraged consumers will take matters into their own hands. Recent privacy tornadoes provide the proof.

For some time, employers have accessed public information from social media sites to monitor employee activities or to investigate the personal qualifications of prospective hires. But recently, companies have gone further, demanding that employees and prospects provide user names and passwords that would enable the company to access otherwise limited distribution material. Dave Johnson, a writer for CBS Money Watch, said employer demands for access to an employee's or prospective hire's Facebook username and password are "hard to see … as anything other than an absolutely unprecedented invasion of privacy."

The reaction was predictable. In the past year, six states – California, Delaware, Illinois, Maryland, Michigan and New Jersey – have reacted to public outcries by outlawing the practice of employers coercing employees into turning over social media account access information. At least eight more states have similar bills pending, including Massachusetts, Minnesota, Missouri, New York, Ohio, Pennsylvania, South Carolina, and Washington. See National Conference of State Legislatures Legislation Summary as of Jan. 8, 2013.

Similarly, Congress enacted the Children's Online Privacy Protection Act (COPPA) in 1998 in response to the failure of self-regulation to limit the scope and nature of information collected from young children. COPPA and implementing regulations limited the collection of information from or about children less than 13 years old. In the past several years, it was widely conceded that this law was not effective in preventing the collection and use of personal information about our children, particularly where photographs and mobile phones were concerned. Companies collecting and using information about children took no action to satisfy parental concerns.

The reaction? In December 2012, the Federal Trade Commission issued amended regulations to make clear that COPPA rules apply to a child-oriented site or service that integrates outside services, such as plug-ins or advertising networks, to collect personal information from visitors. The definition of restricted personal information now includes geolocation as well as photos, videos, and audio files that contain a child's image or voice, and "persistent identifiers" that recognize users over time and across different websites or services.

Parents and job counselors have been warning for years that teenagers and young adults must not post unflattering images to their Facebook pages because, even if deleted, they will persist somewhere on the internet and may be found by prospective colleges and employers. There were many anecdotes about teenagers committing suicide after nasty postings or the distribution of photos. There did not seem to be a practical solution to the problem.

Last year, the European Commission proposed a sweeping revision to its already difficult data privacy rules to include an explicit "right to be forgotten." If the proposal is adopted, individuals can demand that websites remove personal photos or other data. Companies that fail or refuse to do so could be fined an amount based on their annual income. The rules, as proposed, would apply both to information the data subject posted about herself and embarrassing information others posted about her, unless the website can prove to a regulator that the information is part of a legitimate journalistic, literary, or artistic exercise. Such a new law would set up a dramatic clash between the European concept of privacy and the American concept of free speech.

For the past three years we've heard shocking stories about phone Apps that quietly collect information about our searches, interests, contacts, locations, and more without disclosure or a chance to opt out. The uproar led to only limited action that has not satisfied consumer concerns.

The reaction? U.S. Representative Hank Johnson has proposed The Application Privacy, Protection, and Security (APPS) Act of 2013, which would require App developers to disclose their information-gathering practices and allow users to require that their stored information be deleted.

Increasingly, consumers are not waiting for regulatory action, but are taking privacy protection into their own hands. For example, Instagram built a business on its photosharing App. Shortly after it became popular enough to be purchased by Facebook, Instagram issued new terms of service and privacy policies that appeared to give the company the right to use uploaded images without permission and without compensation. The Washington Post described consumer reaction as a "user revolt. . . on Twitter where shock and outrage mixed with fierce declarations swearing off the popular photo-sharing site for good." The Twitter response was so memorable that perhaps, in the future "insta-gram" will come to have a secondary meaning of "a massively parallel instantaneous complaint in cyberspace."

The blogosphere and Twitterterra were filled with apologies and explanations by Instagram and others stating the company was not a bad actor and truly had no intention of using photos of your naked child to sell diapers without your permission. Even some of the harshest critics admitted, "it's [not] quite as dramatic as everyone . . . made it seem like on Twitter." See Theron Humphrey quoted in David Brancaccio's Marketplace Tech Report for December 19, 2012. But the truth about the revised terms and conditions may not matter because consumer goodwill toward Instagram had been destroyed by the perception.

Instagram users are not alone in their disapproval of commercial uses of personal information. Consumer analytics company LoyaltyOne released a July 2012 survey that shows U.S. consumers are increasingly protective of personal information. Of the 1,000 consumers responding, only about 50% said they would be willing to give a trusted company their religious or political affiliation or sexual orientation, only 25% were willing to share commonly commercialized data such as their browsing history, and only 15% were willing to share their smart phone location. USA Today reported that an ISACA survey of adults 18 years and older showed that 35% would not share any personal information if offered 50% off a $100 item, 52% would not share any personal information if offered 50% off a $500 item, and 55% would not share any personal information if offered 50% off a $1,000 item. USA TODAY, *Bigger Discount, Less Sharing*, January 21, 2013.

I'm confident everyone reading this *Update* has been sufficiently careful and prudent in their own personal and professional lives; but who among us has not had an, ahem, *family member*, who does not regret a photo posted to a social media site, an unappreciated email joke, or a comment in a tweet or blog that looks much less "awesomely insightful" after the passage of a few days. (Is there an emoticon meaning "I'm being really facetious"?) Such brief moments of indiscretion can lead to disproportionately bad results.

Have commercial collectors, users, and resellers of such information shown sufficient willingness to respond to consumer's widespread discomfort with the permanent retention and uncontrolled access to their personal information, candid photos, and musings?

We no longer inhabit a Wild West without limit on the collection and use of personal information for commercial purposes. Be assured, that when something perceived to be bad happens, there will be a violent, goodwill damaging, market value destroying, throw-out-the-baby-with-the-bath-water Instagram-like response that will obliterate some current business models and corporate franchises. Notwithstanding terms and conditions of service that try contractually to deprive users of any right to complain about your use of their data, they will complain and they *will* vote, with both their Feet and their Tweets.

There are very good social, psychological, religious, and political reasons why privacy should be protected. *See* Wolfgang Sofsky, PRIVACY: A MANIFESTO (Princeton Univ. Press 2008). As consumers and parents we instinctively know that privacy is important, even if we can't precisely define it and can't say exactly why. Even though we've sometimes been too foolishly willing to let go of privacy protections in exchange for the convenience of a nifty new website or clever new App, we do, in the end, still care. We know there is something important at issue here. We should not forget this insight when we change hats and become business people deciding what data to collect and how to use it.

Companies that want to avoid receiving an "insta-gram," that want to build long term relationships with consumers, need to accept that sentiment has changed when designing their programs, analytics, and business models. It's time to throw out McNealy's aphorism. Businesses need to recognize that today consumers increasingly do value their privacy, and get over it.

---

von Briesen & Roper Legal Update is a periodic publication of von Briesen & Roper, s.c. It is intended for general information purposes for the community and highlights recent changes and developments in the legal area. This publication does not constitute legal advice, and the reader should consult legal counsel to determine how this information applies to any specific situation.