

THURSDAY, AUGUST 28, 2014

PERSPECTIVE

## Online privacy concerns only increasing

By Kimberly Buffington and Carolyn Toto

As the use of the Internet has expanded to permeate every aspect of our lives, so have myriad legal issues. The rapid pace of change has challenged the law in catching up in areas like online privacy. The amount of information being exchanged on the Internet is mind-boggling, and — because so much information can be gleaned from individuals by what they do (often unknowingly) — privacy has become a big concern.

### EU's "Right to Be Forgotten" Decision

This summer, the highest court in the European Union upheld the "right to be forgotten," giving EU citizens the right to request that Google remove any search results that represent an individual in an unflattering way and holding search engine operators responsible for the personal information which appears on webpages published by third parties. Other search engines have followed Google's lead in implementing a take-down process for search results in Europe for queries that include a person's name if the results shown are "inadequate, irrelevant or no longer relevant, or excessive."

There is debate over how the EU's decision should be implemented. EU privacy regulators are meeting with technology firms to discuss contentious issues, such as the breadth of the right to be forgotten. Google has refused to remove name-search results from its primary search engine; only removing name-search results from more jurisdictionally narrow Google pages, such as google.co.uk. Google has also come under fire for posting take-down notices in place of content search results to indicate that certain content has been removed in accordance with the EU law. Privacy officials take the position that allowing Google to do this makes the law ineffective.

The U.S. is not bound by the EU decision, but the right to be forgotten has certainly sparked interest and discussion in the U.S. Since the decision, there has been a surge in websites such as Forget.me offering to help remove unflattering search results from searches of individuals' names. About one-third of the company website's traffic comes from U.S. citizens, which demonstrates that Americans have a high interest in disassociating certain web results from their names.

### Litigation over Bad Yelp Reviews

There has been a recent surge in litigation arising from negative reviews posted on websites such as Yelp. This is an important privacy issue, because people often give reviews freely online, thinking their opinions are protected under the First Amendment and that their identities will never surface if they post an anonymous review. Recent litigation has challenged these expectations. Plaintiffs and courts have only recently begun to test the boundaries of what may not be protected as free speech in an online review.

For example, earlier this year the Virginia Court of Appeals held that Yelp had to find and reveal the identities of anonymous users who had posted negative reviews of a business. The business owner sued the anonymous reviewers because he believed that they were not customers of the business and were thus making false, defamatory statements. The judge explained that customers have the right to express themselves anonymously as opinions under the First Amendment, but that negative reviews posted by people who are not customers constitute false statements rather than protected speech. The Virginia Supreme Court agreed to hear Yelp's appeal and the case is likely to go before justices in Richmond in the next few months.

Depending on the outcomes of this case, and others like it, people may become more apprehensive about publishing reviews online

### Mugshot Publishing Industry Shakedown

In recent years, an online mugshot publishing industry has developed, with websites making money by charging significant fees to individuals who want their mugshots removed from a website. These websites often include old mugshots, even after charges are dropped or the subject of the mugshot has been found innocent. While mugshots are public records, the mugshot industry alters the extent to which a person's mugshots are accessible by making mugshots pervasive in Google searches and charging hefty fees for removal.

Some have said that the industry capitalizes on, and exacerbates, socioeconomic inequalities by giving the wealthy a way to mitigate the impact of their mugshots on their lives while depriving the less wealthy of any remedy. In effect, the industry makes privacy inaccessible to many by charging a premium for it.

This privacy issue has led to recent state legislation attempting to restrict commercial use of public mugshots. Wyoming, Georgia and Utah have all passed measures that outlaw the fee-for-removal practice, and at least 12 other states have mug shot-related bills pending.

### Snapchat's Not-So-Disappearing Photos

Snapchat's app promises to make photos, messages and videos sent to other users vanish after a specified time period. However, it was recently revealed that the sent data is not fully removed as promised and the company routinely gives data to the government. Because Snapchat is an application that often revolves around potentially sensitive user data and photos, users might not have chosen to use Snapchat if not for its representation to users that the data and photos disappear after a limited time.

In January, hackers exposed the usernames and phone numbers of 4.6 million Snapchat users after the company ignored security researchers' warnings about a flaw in the app's security potentially enabling theft of personal data. In May, Snapchat settled charges by the U.S. Federal Trade Commission that the company was deceptive in representing that messages sent through the app disappear and in misrepresenting its data collection practices. Given Snapchat's gain in popularity and use, the increased scrutiny by regulators of its privacy practices signals a similar trend through the industry.

### "Canvas Fingerprinting"

Websites ranging from Whitehouse.gov to YouPorn now employ a new online tracking method called "canvas fingerprinting." Developed to serve as an alternative to cookies, canvas fingerprinting helps websites uniquely identify and track visitors by "shadowing" them. The tracking method tells browsers to draw a hidden image specific to one's browser, operating system and graphics driver that is turned into a digital "token" which is then used to create a profile for the user to provide better targeted ads. This tool raises privacy concerns because canvas fingerprinting is invasive, most users are not aware of it, and it cannot be prevented by ad blockers or incognito browsing. Researchers from Princeton and KU Leuven University estimate that 5 percent of the most popular websites utilize canvas fingerprinting. Because the numbers will only grow, it will be interesting to see

how the public (and regulators) react as more people learn about the tool.

### I Know Where Your Cat Lives

"I Know Where Your Cat Lives" is a data experiment aimed to demonstrate the volume of personal data individual users leave throughout the web by plotting cat locations from metadata from public files on the Internet. The images are gathered from public image posting websites like Flickr and Instagram. The project reveals cats' and their owners' locations up to an estimated 7.8 meters, creating awareness of the amount of data we reveal in our "daily digital lives." This project and the concept of geotracking demonstrate the extent to which location-based data permeate individuals' online activities. For example, many social media programs like Twitter have geotagging settings that may be applied to a user's account unknowingly, implicating that user's privacy by revealing his or her location to the world.

### Tracking Online Browsing History

Google is purportedly developing an alternative to cookies on its Chrome browser — an anonymous identifier, or AdID — to track user's online browsing activity. The new alternative is also said to give users the ability to limit ad tracking through browsing settings and may be reset every year by the user. Advertisers will be allowed access to the AdID's so long as they adhere some basic guidelines. It appears that the proposed changes will give users the ability to choose how their online activity is tracked may give more privacy and control. Those in the advertising industry, however, are wary because the proposed system may be shifting more power and control away from advertisers to Google.

**Kimberly Buffington and Carolyn Toto** are partners in Pillsbury Winthrop Shaw Pittman LLP's Los Angeles office.



KIMBERLY BUFFINGTON  
Pillsbury Winthrop

CAROLYN TOTO  
Pillsbury Winthrop