ADAM BERRY/GETTY IMAGES

# What we talk about when we talk about privacy

BY STASH LUCZKIW

The internet has blasted open a Pandora's box of personal space. The EU's recent decision to allow Google users the right to be forgotten highlights ongoing tensions in an attempt to balance freedom of expression and privacy.

**Pieces of candy featuring the Google logo.**

When most people imagine criminal misuse of private data on the internet they usually think of identity theft. The scenario is fairly straightforward: you have given your information – name, date of birth, credit card number, email – to an online charity for helping single mothers in Latin America. You've also given the same information to an online travel agent, a cable television company, and a manufacturer of crushed velvet cat cushions. Later the same month, your credit card company notifies you that suspicious debits from a dubious online marriage counseling service have appeared on the same credit card and you are advised to block the card immediately.

This is one of the more prosaic examples. Another, trickier situation could play out as follows: You live in Berlin, somewhat happily married, but are having a secret affair with a man or woman in Hannover. You told your spouse that you were in Warsaw over the weekend because you had to visit clients. Your spouse, who up till now has refused to become suspicious, is solicited by a new online service called Big Sister, which tracks down all public records available about any given person. Your spouse tries it out, enters your name and telephone number. Among the data that Big Sister spits out is a speeding ticket issued in Hannover for the very weekend you said you were in Warsaw. Now you have a lot of explaining to do.

Yet another hypothetical scenario: You are HIV positive and have been scouring the internet for natural treatments to boost your immune system. You have been researching the availability of drugs in various countries in the hope of saving money. Many years later, your insurance company finds out about your

JACQUES DEMARTHON/AFP/GETTY IMAGES

**President of France's leading consumer rights group, UFC-Que Choisir, Alain Bazot (L) and the editor in chief of monthly magazine *Que Choisir* Jean-Paul Geai (R) pose in a Paris office, March 25, 2014.**

searches and purchases, and has you take another blood test. The first time you took it, for some miraculous reason, it came out a false negative, despite the fact that you knew you were positive. Now the insurance company, which got your search information from a company similar to Big Sister, says they intend to reevaluate your status.

The first example is a fairly common occurrence, and the existence of identity theft via the internet has spawned a booming internet security industry. The latter two examples, while far-fetched, are by no means science fiction. All three examples highlight what has become one of the most crucial debates in the context of the Information Revolution: with such easy access to so much information, combined with the computing technology to gather and parse it all for very specific ends, where do we draw the limits as to what type of private information can and cannot be used?

With the public revelation in 2013 that the US National Security Agency and secret services of other nations have been tapping into data provided by phone and internet companies, the debate has become more heated and legislators have been forced to enter the data privacy fray. Most recently the European Court of Justice (ECJ) ruled in May that citizens do have a certain "right to be forgotten" online. The court ordered Google to remove links to archived newspaper pages containing old information about the repossessed home of a Spanish man, who sued Google and the newspaper in 2010. Google will have to remove some search results upon request because the court believes that old information about a person can be not only irrelevant but also misleading. The ECJ ruled that a search engine like Google has a responsibility to delete links concerning personal information upon request as long as that information is not relevant or in the public interest. Since the ruling, individuals in Europe hoping to have search results deleted have sent Google an average of 10,000 requests per day, or one every 7 seconds, according to *Time* magazine.

However if developments up till now are any indication, they will always be the tail wagging behind the juggernaut of the computer cloud. In an interview with Italian daily *Corriere della Sera*, Google CEO Eric Schmidt said that they were stunned by the court's decision. "It's a delicate balance between the right to be forgotten and the right to know, and we believe the court found the balance in the wrong place." Nevertheless, the internet colossus intends to hire more personnel to vet the flood of requests to be forgotten.

Privacy is one of those terms that on the surface seems to need little explanation. It involves maintaining the sanctity of the individual and the individual's personal space, information, image, property. However, in order to establish which aspects of privacy merit legal protection we are forced to explore its nuances. With the advent of the internet, all our notions of space and image have been irredeemably warped by the breathtaking speed with which unfathomable quantities of information are processed and the range of its transmission.

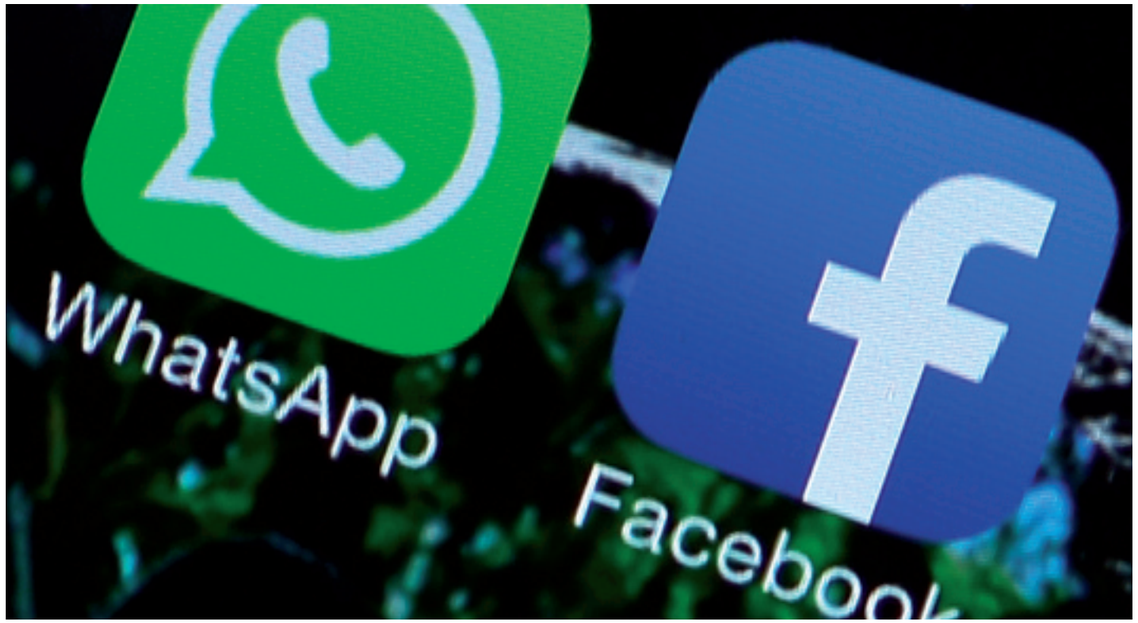
Now, in the age of Google, data has become an extremely lucrative commodity. As a result, data privacy has become one of the stickiest legal issues in town – a town that is now, as Canadian sociologist Marshall McLuhan had already predicted in the 1960s, a veritable "global village."

Some of the most glaring privacy issues that have come to the fore stem from cultural differences. The notion of privacy as an inherent individual right is very much a Western concept, which developed over centuries of Greco-Roman and Christian culture. Asians and Africans also have their own protocols with respect to personal space, but privacy as such is not considered an inalienable human right.

Even in the West there are significant differences in








GABRIEL BOUYS/AFP/GETTY IMAGES

**The Facebook and WhatsApp icons displayed on a smartphone.**

how privacy is viewed between Europeans and Americans. In his 2004 essay on the subject, "The Two Western Cultures of Privacy: Dignity Versus Liberty," James Q. Whitman, professor of comparative and foreign law at Yale University, writes: "European and American sensibilities about privacy grow out of much larger and much older differences in social and political traditions. The fundamental contrast, in my view, is not difficult to identify… Continental privacy protections are, at their core, a form of protection of a right to *respect* and personal *dignity*."

Europeans tend to interpret privacy as their right to control their public image, name and reputation. They expect to be shielded from unwanted public exposure, to be spared embarrassment or humiliation. "The prime enemy of our privacy, according to this continental conception, is the media, which always threatens to broadcast unsavory information about us in ways that endanger our public dignity." The media, of course, has now come to include the internet; and the internet's increased potential for broadcasting unsavory information has put European privacy watchdogs on alert.

"By contrast," Whitman goes on, "America, in this as in so many things, is much more oriented toward values of liberty, and especially liberty against the state. At its conceptual core, the American right to privacy still takes much the form that it took in the 18th century: It is the right to freedom from intrusions by the state, especially in one's own home." The prime danger, from the American point of view, is that the private sovereignty of the home will be breached. Hence the almost fanatical insistence on the right to bear arms."

This contrast has created headaches for global data businesses, such as Google. Since its meteoric rise as a paragon of the information economy, Google has been under attack for what is seen as a fast and loose privacy policy, especially in Europe.

In 2010 Google's "Street View" camera vans came under scrutiny by French regulators because they were gathering information from wifi networks, and some of that information may have included passwords and other data covered by banking and medical privacy regulations. Google blamed the collection on a rogue bit of code that was never removed after it had been inserted by an engineer during testing.

In the same year, when Google came out with Buzz, a social networking platform meant to compete with Facebook, the search engine was savaged by privacy advocates for making email addresses (often very private ones, such as those of doctors, lawyers and lovers) available to others without permission. Google had to quickly correct the flaw to avoid a public relations fiasco.

Facebook has also been pummeled by privacy advocates. Since its main asset is the vast data with regard to users' interests and "likes" contained in their "social

JUSTIN SULLIVAN/GETTY IMAGES

A young woman wears Google Glass at an unrelated book presentation and media event on June 10, 2014 in Berlin, Germany. Google Glass, which films what the wearer sees and has a connection to the internet, has caused controversy with privacy advocates.

graphs," Facebook's every move is being watched.

Another case that spotlighted the transatlantic divide when it comes to notions of privacy was the Vivi Down v. Google case in Italy (Vivi Down is an advocacy organization for sufferers of Down Syndrome). In February 2010, three Google executives were condemned for breach of privacy because in 2006 YouTube, owned by Google, allowed a video to be uploaded in which an autistic boy was being bullied. Even though the video was removed shortly after YouTube was notified of its offensive content, an Italian Judge deemed it negligent in notifying those who uploaded data as to the legal privacy risks they ran. Then in 2012, the court of appeals overturned the decision and exonerated Google, or any other server, of responsibility. All the same, the case sparked a debate that rippled throughout the European Union.

In response to the original sentence, William Echikson, Google's head of free expression policy and PR, Europe, Middle East & Africa (a position that had previously been called "communications manager"), vehemently refused to acknowledge the issue as one of privacy. "This has nothing to do with privacy," he insisted. When asked what the case was about, he responded flatly, "This is about freedom of expression." Then, after giving it a bit more thought, Echikson nuanced the response: "This is about who is responsible."

In the wake of the initial condemnation, Nicole Wong, who was then vice president and deputy general counsel at Google and now works as legal director for Twitter, noted the commercial difficulties faced by a borderless internet company having to contend with contradictory jurisdictions. In *The New York Times* she pointed out: "The framework in Europe is of privacy as a human-dignity right. As enforced in the US it's a consumer-protection right." Wong felt that Google's policies on invasion of privacy, like its policies on hate speech, pornography and extreme violence, were best applied uniformly around the world. Trying to meet all the differing local standards "will make you tear your hair out and be paralyzed."

Indeed, the simple fact that service providers that can be based in virtually any country makes it difficult to expect them to adhere to the laws of the EU. According to Alexandra Neri, a Paris-based lawyer for Herbert Smith Freehills, who has advised Google in French intellectual property matters, "One of the biggest issues facing businesses, legislators and lawyers with respect to data privacy relates to cross-border personal data flows, which happen on a massive scale and on a daily basis 'in real life.' Within the issue of personal data protection, international data transfers are unquestionably an area that needs to evolve. Companies are global, as are the IT systems sustaining their businesses."

But is it possible to come up with a global standard for internet data privacy? If so – and there are many who doubt it (just look at how well the US and Britain have managed to adopt the indisputably more efficient metric system) – who will lead the way? The US or Europe?

"European regulations are certainly demanding in terms of personal data protection, creating a high level of protection," says Neri. "Although the restrictions on exporting data outside the EU have undoubtedly contributed toward raising the 'adequate level of protection' on a global basis, they have also created a burden on European companies. Binding corporate rules and data transfer agreements are not truly adapted to dealing with data transfers given the time and energy required to set them up, not to mention obtaining the necessary approvals… More flexibility will certainly be required to fill in the gaps between legal systems in competition around the globe."

While the internet has in many ways magnified already existing legal issues, there is one matter that appears to have been created ex novo with the arrival of

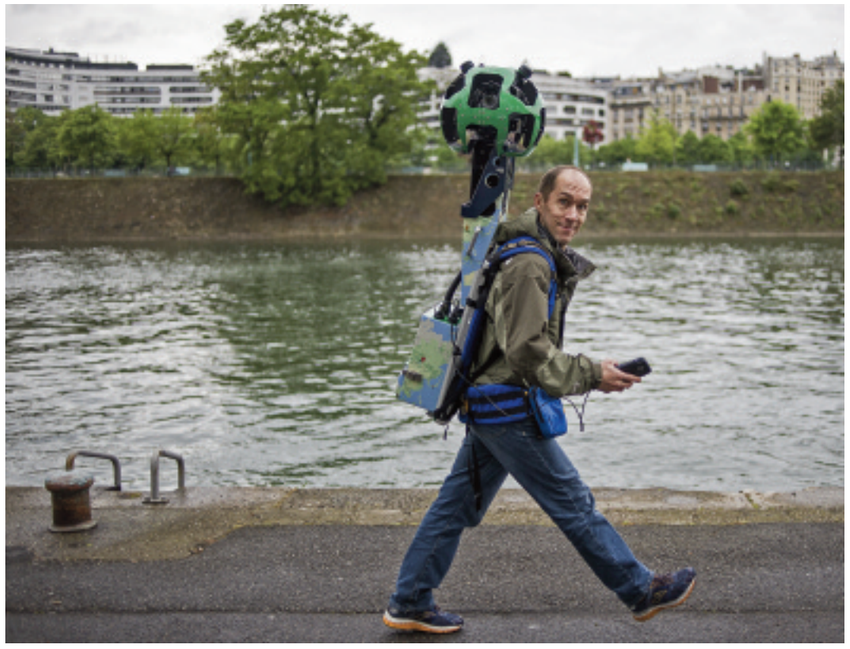




Google and Facebook: the right to be forgotten, or erasure of data. In other words, can any unsavory information "out there" on the internet be expected to be erased? Or will it stay there for eternity?

Here is where the privacy issue can bleed into defamation. Bloggers are notorious for disseminating specious facts and spurious claims. But nowadays, established newspapers are increasingly read online, and they have adopted the blog format of instantaneous opinion-mongering.

But what happens in the following fictitious example? In 2006 John Doe was convicted of fraud. His name was splashed across cyberspace as a white-collar criminal. Then, two years later, he was acquitted in the appeals court because new evidence had popped up in the interim and determined that he was not only innocent, but had been framed. If anyone searches his name on Google, the conviction turns up higher on the page (thanks to the search engine's somewhat esoteric page ranking algorithms) than does the subsequent acquittal. Therefore, in the future, if any prospective employer decides to Google John Doe, the unsavory news may jeopardize his livelihood.



FRED DUFOUR/AFP/GETTY IMAGES

French engineer Luc Vincent, in charge of all the imagery in Google's online maps, walks through Paris carrying the custom-made panoramic camera which has made Google's Street View possible, April 25, 2014.

This type of situation begs the question: Does Mr. Doe have a right to have his data erased? And if he does, to what extent? The ECJ has ruled that "if, following a search made on the basis of a person's name, the list of results displays a link to a web page which contains information on the person in question, that data subject may approach the operator directly and, where the operator does not grant his request, bring the matter before the competent authorities in order to obtain, under certain conditions, the removal of that link from the list of results."

Still, there is plenty of interpretive wiggle room. The right can be denied if it goes against the public interest. Also, critics claim that if such a regulation is interpreted loosely, then only those with the financial means to pursue legal action can benefit. If the regulation is enforced strictly, then it can lead to preventive censorship, similar to what exists in China. There is also the matter of a time limit as to how long a server can hold on to certain information before it is required to erase it. As such the right to be forgotten promises to become not only a prominent legal issue in the near future, but in many respects an ontological one as well.

So whether you are an IT evangelist who sees human progress growing exponentially as a result of the Information Revolution or a skeptical luddite with cyberpunk visions of Big Brother co-opting our very humanity, one thing is beyond a doubt: Barring any cataclysmic return to the Stone Age, the effect Big Data has on our lives is enormous and irreversible.

What this means for us is that we must reevaluate our whole notion of information – and, therefore, epistemology. But the catalyst for such stock-taking is almost always conflict. We are getting a glimpse of this now in the conflict that has arisen between freedom of expression and the right to privacy that ensures our dignity. We will see more of it in the biotech industry as the field of genomics expands and the very building blocks of life become a commodity. In the meantime, governments continue the balancing act between increasing the fruits of the ongoing Information Revolution and keeping it from undermining the humanity it was initially intended to nurture.

STASH LUCZKIW *is a social commentator who covered intellectual property and data protection issues for* TopLegal International.