October 2010

Understanding the "right to be forgotten" in a digital world

By Jennifer L. Saunders

There are at least two opposing points of view when it comes to data retention, and they may well be at the core of many privacy debates across the globe. At issue is the idea of the "right to be forgotten," which has been talked about in many nations and at many levels of privacy discourse, and was illustrated one year ago when two French lawmakers introduced a bill that would give individuals that very right.

Bruno Rasle, executive director of the AFCDP (French Association of Data Protection Correspondents), explains that the phrase the "right to be forgotten" can be construed in two ways, which causes some confusion.

"In the first sense, the 'right to be forgotten' is a prohibition, made in France, against the indefinite retention of personal data. The French Data Protection Act (Informatique et Libertés Law) requires the data controller to define a retention period compatible with the intended purpose," he says.

The CNIL has made some recommendations, and the AFCDP has created a special working group to determine appropriate retention periods, he explains, noting that the CNIL's reference to the "right to be forgotten" relates to the all-too-rare occurrence of the purging of personal data. In reality, he says, there is no "right to be forgotten," as such, in French law.

The second meaning, Rasle suggests, is the right to rectification and objection.

"Some people wrongly interpret these last two rights as an opportunity for them to demand of the data controller, at all times, to erase all personal information about them," he explains. "In fact, the data controller is obliged to delete data only if they are inaccurate, outdated or whose collection is prohibited."

Hunton & Williams LLP Senior Policy Advisor Marty Abrams adds that there is a difference between the idea of a "right to be forgotten" and a "right not to be seen."

In the offline world, he notes, humanity has had "thousands of years to hone this," but online, "the ability to be forgotten and the ability to be unseen have been lost."

The norms around the idea of being unseen in the offline world do not yet translate online, he points out, using the analogy of a domicile as a protected space where individuals live out the private moments of their lives and keep personal belongings, photographs and information. In the online world, the equivalent is a personal computer, where many people store their personal financial information, family photographs, personal writings, book purchases, movie preferences and other private information.

"The books that I read are private to me, but are they private to me when they're sitting on a digital device?" he asks, suggesting our personal computers have, in many ways, become more of a reflection of who we are than our homes, but privacy protection does not extend to these online

spaces in the same way.

This "freedom to observe" data and processes is an American concept, steeped in the constitutional right of freedom of expression, he notes. "In Europe, every step of data is processing, and processing needs a legal basis."

This desire to be forgotten parallels the point of view of those who believe the digital history we create online--sometimes intentionally, and sometimes without even realizing it--should be allowed to "fade away" through a process called data degradation. Then, there is the other side to the argument, the perspective that data must be stored and maintained, either to protect it or as part of a business plan that relies on what has come to be seen as a key commodity: online clicks, posts and visits that can paint pictures of Web users' likes and dislikes.

As technology professional Sean Gallagher writes for *internet evolution* on data degradation, "Chances are that you've left a considerable electronic trail behind you in your travels across the Internet. Your e-mail address, mailing address, birth date, age, credit card numbers, and more are all stored in scores of e-commerce systems, social networking sites and maybe even a job board or two. And your business likely has a trove of similar data about everyone you've ever done a transaction with over the Web."

Although sharing different views on how data should be managed, both Jeff Chester of the Center for Digital Democracy and Linda Woolley of the Digital Marketing Association, for example, spoke of the value of data during a recent appearance on *CSPAN*'s "The Communicators" series.

"Consumers have to understand personal data is a commodity," Woolley said, while Chester noted that what people do online is "the new currency...Data is power."

When it comes to managing what both sides seem to agree is valuable data, such distinct views--to keep or to delete--prompt questions as to whether there's room for compromise or the natural course of events will be for these opposing forces to collide.

As Winston Maxwell notes in a report on the French proposal for the Hogan Lovells Chronicle of Data Protection, the proposal was aimed in part at facilitating data subjects' ability to request the deletion of their personal data as "part of a broader French government campaign to create a citizen's 'right to be forgotten' on digital networks."

On that subject, Rasle refers to concerns voiced recently by the CNIL's president, Alex Türk, on cloud computing, where the "dissemination and duplication of personal data make him fear that, despite the purges, personal data never really disappear and could reappear one day or another."

Data degradation, however, as Gallagher points out in his report, "is the exact opposite of what most IT managers strive to do with customer data," as it is an asset that can be used in myriad ways.

In terms of maintaining or deleting data, Rasle notes, "In reality, these rights depend strongly on the quality of information that was issued by the data controller" to ensure that individuals are "aware of the real implications of collection and also about their rights."

Rasle points to recent comments by European Commissioner Viviane Reding, who has said, "Transparency must be strictly applied."

As Gallagher writes in his report, "For most uses beyond the transactional relationship with customers, we don't need high-resolution data. Often, the data can be 'anonymized' to a large degree for the purposes of larger analytical tasks, and there's definitely a shelf-life attached to the value of data for any given transaction."

Abrams, meanwhile, points to the use of analytics as taking the issue beyond data itself to the idea of process degradation and integrity.

"In a world where every piece of information is feeding into analytic processes that predict future behavior or future outcomes, then the existing data protection principles don't encompass the privacy risks that come from the use of information in predictive processes," he explains. "The information can be sound, and the information can still be relevant, but when put into an analytic process, can lead to outcomes that come to the heart of privacy."

As every analytic model has a failure rate and can lose predictive value over time, it is impossible to consider online data without considering process factors.

"When you think of the impact of information," Abrams says, "you have to really think of it in terms of advanced analytics."
When it comes to balancing issues of data degradation and preservation, Rasle says it will be chief privacy officers playing a crucial role to "ensure the company listens to the people concerned, that their rights are recognized, that their information is assured" and to champion privacy by design and data minimization.

Or, put another way, he says, the "easiest personal data to forget are those we never collected."

This article was published in the October issue of the International Association of Privacy Professionals' Inside 1to1: Privacy *newsletter. For more information visit www.privacyassociation.org.*