PERSPECTIVE

What the "right to be forgotten" means for privacy in a digital age

Abraham L. Newman*

Despite the attention the right has received, we should not forget that it is just one innovative piece of a comprehensive privacy framework that must be implemented locally and enforced globally.

Has Europe upended Internet privacy and free speech with its decision to create a "right to be forgotten"? In May 2014, the European Court of Justice ruled that European citizens have the right to request that search engines delink results to items that are considered inaccurate, irrelevant, or excessive (*1*). In the specific case, a Spanish citizen asked that Google remove a link to a newspaper account of his home foreclosure, a debt he had subsequently paid. In essence, this right acknowledges the stickiness of digital footprints. Photos, court records, and letters that used to get lost in file cabinets are neatly organized and accessible from our laptops. A childhood foible can haunt someone for a lifetime. The right reasserts our human instinct for redemption and forgiveness in the digital age (*2*).

This debate matters not only for how individuals use the right to be forgotten but also as a window into privacy protection more generally. In this essay, I review the controversies surrounding the European decision, describe where the right fits into a broader privacy protection framework, and discuss several implications of the debate. In particular, I argue that the right to be forgotten highlights differences in privacy protection across the globe, marks the emergence of distributed regulatory approaches, and underscores the importance of the international context for successful privacy policy.

Critics of the ruling claim that it will bring the demise of everything from Internet search to free speech (*3*). Search firms will be saddled with the excessive costs associated with processing requests to remove links, and individuals who exercise the right will disrupt free expression by altering search results. In the first five months since the ruling, Google has processed roughly 180,000 requests of which it accepted 40% (*4*). Although review requests are no doubt cumbersome for search firms, they do not appear to pose an insurmountable technical or financial burden. Google's stock in December 2014 is close to its 5-year high and enjoys a market capitalization at over $360 billion. Search firms from Google to DuckDuckGo must be prepared to respond to takedown requests ranging from libel and defamation to copyright, which far outpace the right to be forgotten. In the week of 1 December 2014, for example, Google received copyright takedown requests concerning more than 9 million links (*4*).

In terms of free speech, the European Court decision did not create a right that trumps all others but explicitly called for a balance between the right to be forgotten and other interests. Moreover, the effect of the decision on speech is limited as it does not require the deletion of the original content but rather the delinking of that content from search results. It takes us back to a world where people might have to go to a city hall or library to research past debts rather than instantly downloading them.

The stakes of data correction for consumers can be high. A 2012 study by the Federal Trade Commission in the United States estimates that one in four individuals have an error in their credit report that could affect their credit score (*5*). A 2014 lawsuit filed by the State of Mississippi against Experian, one of the largest credit reporting agencies in the United States, suggests that Experian produces reports with errors and that consumers have considerable difficulty correcting them (*6*). These errors affect the ability of millions of Americans to get competitive interest rates for home and auto loans, obtain security clearances, or pass rental applications.

When considering a privacy framework, however, rules about data correction and erasure are just one piece of the puzzle. Equally vital, if not more important, are rules that govern how data can be collected and then used by other parties that were not involved in the original data collection. Can a company like Uber (the app-based transportation network and taxi company) collect and store location data from individuals as they use their services; can those data be used for purposes other than securing transportation; can it then share that data with other companies or the government; and can it store data even after a customer has cancelled an account? The right to be forgotten is just one piece of a comprehensive data privacy framework that would include rules surrounding data collection and how data are then used, analyzed, shared, and secured (*7*).

Privacy is not dead

The right to be forgotten is a potent reminder that Europe has developed such a comprehensive approach and stands in sharp contrast to U.S. privacy policies. The European Court of Justice's decision builds upon a coherent and robust privacy framework in both the European Union and its member countries that includes rules concerning the collection, use, and storage of personal data in the public and private sector. These rules are overseen by independent national regulatory agencies known as data privacy authorities. Originally, the regulations were based in national laws dating back to the 1970s, but the European Union has taken on a greater role in this domain since the passage of the Data Privacy Directive in 1995 (*8*). In this system, big players like eBay or IBM work closely with regulators and implement internal data privacy policies in order to prevent data privacy scandals (*9*).

In contrast to the European system, the United States has a fragmented, patchwork approach to privacy regulation. With the passage of the Privacy Act in 1973, the United States focused privacy rules on data collection by the federal government along with a limited number of regulations covering a varied and idiosyncratic set of private-sector activities. The United States is notorious for having stronger privacy protections for video rentals than online marketing. Moreover, as the lines between sectors such as telecommunications, marketing, and finance merge, such divisions become less and less tenable. Equally important, there is no single regulator dedicated to overseeing the implementation and enforcement of disparate regulations (*10*).

The different approaches to privacy in Europe and the United States shape how governments and firms process and share personal information. In the United States, for example, nearly 100% of the population has a private-sector credit report, including "positive" information ranging from income to purchasing patterns. These types of data are routinely used to construct predictive scores such as the Consumer Profitability Score or the Individual Health Risk Score (*11*). In France, roughly 3% of the population has a credit report, which details "negative" information, such as defaults or missed payments, and as a result, there are far fewer predictive scores (*12*). European privacy rules are not a panacea for the immense challenges posed by digital technologies, but they offer a strikingly different set of ground rules from which to begin the debate.

Distributed regulation

The right to be forgotten is part of a trend in privacy protection toward distributed regulation, in which regulators rely on individuals and firms to monitor and implement regulations. Such legislation leverages the large number of consumers across the economy to be part of the regulatory process. Transparency, accountability, and class-action remedies encourage consumer advocacy groups to organize and hold firms and governments accountable to the rules.

At the same time as consumer groups press for action (*13*), private firms increasingly carry out remedies. Companies, such as Google or Microsoft, have been deputized (in consultation with data privacy authorities) to evaluate and implement

Associate Professor in the Edmund A. Walsh School of Foreign Service at Georgetown University, Washington, DC 20057, USA.
***Corresponding author. E-mail: aln24@georgetown.edu**

delinking requests. Whereas involving companies in the solutions has the benefit of distributing the task of enforcement, it raises the real risk of delegating sensitive issues like free speech regulation to corporations.

The right to be forgotten's emphasis on distributed regulation is similar to data breach laws that emerged from state-level experimentation in the United States. These laws require firms to notify customers when their personal data have been lost or stolen. California was among the first jurisdictions to adopt such rules in 2002, which have now spread to all U.S. states except Alabama, New Mexico, and South Dakota. Europe adopted similar rules in 2013 for telecommunications and Internet service providers and will pass more encompassing rules as part of the General Data Protection Regulation, which will be adopted in 2015 (*14*). These laws have had a number of important impacts. Firms that encrypt their data are exempt from notification requirements, and so they have increased the use of encryptions. And although critics have argued that consumers may become fatigued by notices, data breach rules have raised the salience of the issue to a top-level executive concern that might have previously been squirrelled away in an information technology department. Finally, they put firms in the position of providing an important remedy by making credit report checks available to affected customers (*15*). These distributed regulatory policies do not eliminate more traditional forms of regulation, such as direct oversight or sanction, but expand the toolbox.

Privacy goes global

Describing the European and U.S. approaches to privacy separately misses the important ways in which data protection is increasingly international. In today's digital world, information flows routinely cross borders, and such data flows are carried out by a handful of large technology and telecommunications firms. Citizens from Germany to Brazil must trust largely American companies like Google or Cisco to protect their privacy rights.

The right to be forgotten demonstrates the limits of national data privacy systems in a world of transnational data flows. In the wake of the European Court of Justice decision, once a delinking request has been approved, Google removes the link in the national domain name environment (for example, google.de, in Germany), while maintaining the link in other domains (such as the global google.com). Critics have argued that this negates the right as the offending information is still available on other domain name platforms. In November 2014, European privacy regulators made this concern official by recommending that companies respect such right-to-be-forgotten decisions globally (*16*) (Fig. 1).

The mismatch between regulatory jurisdiction and the transnational flow of information is a much more general phenomenon that plagues privacy protection. As revealed by the recent scandal involving the U.S. National Security Agency (NSA), personal data are often transmitted across networks that span countries. As companies employ more sophisticated surveillance techniques such as Super Cookies (*17*), these concerns are not limited to covert government activity. Data havens could emerge similar to tax havens, in which firms store data in jurisdictions with weak privacy rules.

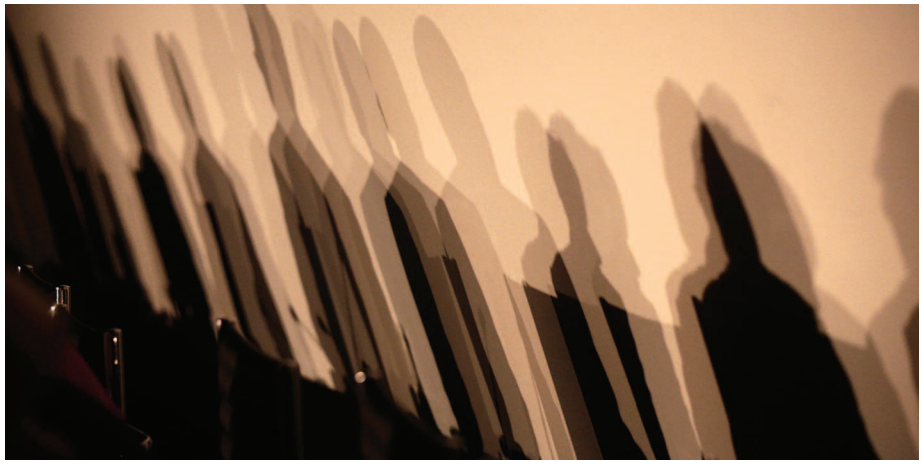

Fig. 1. How long will digital shadows remain? Shadows of members of a panel are seen on a wall before a meeting about the "right to be forgotten," in Madrid, 9 September 2014. [REUTERS/ANDREA COMAS]

To address these challenges, Europe has attempted to extend its jurisdiction beyond its borders (*8*). An important component of the European privacy system is that it limits data transfers to jurisdictions like the United States that do not have "adequate" protections in place. This has led many major information technology firms, such as Amazon and Google, to quarantine data about European citizens within European data centers. The NSA scandal has accelerated this trend, with U.S.-based cloud computing firms, for example, expecting to lose 20% of their business in foreign markets (*18*). In other words, the regulation of U.S. information technology companies is increasingly being set in Berlin or Brussels.

The right to be forgotten has energized a debate concerning privacy on the Internet. In particular, it has the potential to mobilize consumers to become involved in the process and to provide a new way to minimize the harms associated with the publicity of inaccurate or outdated information. At the same time, it needs to be kept in context of a broader privacy framework that considers how personal information is collected, shared, used, and secured. The European model offers one such approach. And that approach has been widely adopted outside of the United States in countries ranging from Canada to Argentina (*8*). National or regional privacy solutions, however, will face considerable difficulties if other countries, like the United States, maintain weak privacy systems that give safe haven to data brokers. Distributed regulatory tools, such as the right to be forgotten, as well as the broader comprehensive privacy framework's success will depend in large part on Europe's commitment to defending its system globally even if that means enforcing its rules across borders and periodically taking U.S. firms to task.

REFERENCES

1. European Commission, "Factsheet on the 'right to be forgotten' ruling" (C-131/12, EC, Brussels, 2014); http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf
2. V. Mayer-Schonberger, *Delete: The Virtues of Forgetting in the Digital Age* (Princeton Univ. Press, Princeton, NJ, 2011).
3. Editors, *New York Times*, 14 May 2014, p. A26; http://nyti.ms/1tOQdiJ.
4. Google, Transparency Report: European Privacy Requests for Search Removals (Google, 2014); https://www.google.com/transparencyreport/removals/europeprivacy/?hl=en.
5. Federal Trade Commission, "Report to Congress under section 319 of the Fair and Accurate Credit Transaction Act of 2003" (FTC, Washington, DC, 2012).
6. J. Horwitz, *Columbus Dispatch*, 17 June 2014; http://bit.ly/1yAX1Bt.
7. D. Solove, P. Schwartz, *Information Privacy Law* (Wolters Kluwer, New York, 2014).
8. A. Newman, *Protectors of Privacy: Regulating Personal Data in the Global Economy* (Cornell Univ. Press, Ithaca, NY, 2008).
9. F. Bignami, *Am. J. Comp. Law* **59**, 411–461 (2011).
10. P. Regan, *Legislating Privacy: Technology, Social Values, and Public Policy* (Univ. of North Carolina Press, Raleigh, 1995).
11. P. Dixon, R. Gellman, "The scoring of America: How secret consumer scores threaten your privacy and your future" (World Privacy Forum, San Diego, CA, 2014).
12. N. Jentzsch, *Financial Privacy: An International Comparison of Credit Reporting Systems* (Springer, Berlin, 2007).
13. C. Bennett, *Privacy Advocates: Resisting the Spread of Surveillance* (MIT Press, Cambridge, MA, 2008).
14. European Commission, Commission proposes comprehensive reform of data protection rules [news release] (EC, Brussels, 2012); http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm.
15. Experian, "Data breach industry forecasts" (Experian, Costa Mesa, CA, 2015); www.experian.com/assets/data-breach/white-papers/2015-industry-forecast-experian.pdf?_ga=1.172114915.1943093614.1418003182.
16. S. Schechner, F. Robinson, *Wall Street Journal*, 26 November 2014; http://on.wsj.com/1xFhvI4.
17. C. Timberg, *Washington Post*, 3 November 2014; http://wapo.st/1FnxzmQ.
18. C. Miller, *New York Times*, 22 March 2014), p. A1; http://nyti.ms/141KBEY.

10.1126/science.aaa4603