DOES THE U.S. NEED A "RIGHT TO BE FORGOTTEN"?

By Attorney Kimberly A. W. Peaslee

Electronically stored and electronically indexed information is ubiquitous. We are arguably living in the age of the “internet of things,” where everyone and everything is traceable online. With technology moving so fast, it is hard to picture what our interaction with information looked like a decade ago or what our interaction with information will look like ten years from now. In fact, that is part of the controversy surrounding the Court of Justice of the European Union’s (the “CJEU”) recent application of the 1995 European Data Protection Directive (“the EU Directive”) in the Google Spain case.1

While the Google Spain case is interesting on a number of levels, the focus of this article will be on whether the U.S. should consider legislation similar to the EU Directive, which has become known as “the right to be forgotten,” or whether there is a more appropriate solution. Any U.S. solution will need to balance an individual’s interest in their personal data with the preservation of others’ First Amendment rights.

THE EU DIRECTIVE

The EU Directive regulates the processing of “personal data” within the European Union. “Personal data” is defined as “any information relating to an identified or identifiable natural person, hereafter referred to as a “data subject”. The responsibility of ensuring the proper processing of “personal data” rests on the “data controller.”

There are several overarching principles in the EU Directive that provide for the processing of personal data. Appropriate processing must be transparent, serve a legitimate purpose, and be proportional to the purpose for which it was collected. As a general notion, the data subject must be informed that his or her personal data is being processed. Article 6 of the EU Directive provides that data must be “adequate, relevant, and not excessive” in relation to the purposes for which it was collected. The data must also be accurate and not kept “longer than is necessary.” Article 12 of the EU Directive provides that a data subject can request that a data controller rectify, erase, or block data if it does not comply with the provisions of the EU Directive.2

THE GOOGLE SPAIN CASE

Google Spain, decided late in 2014, dealt with a Spanish citizen, Mr. Gonzalez, who sued Google Spain seeking the removal of links to La Vanguardia newspaper announcements about the foreclosure on his home due to unpaid debts.3 Announcements pertaining to Gonzalez were initially published in La Vanguardia in 1998. Mr. Gonzalez objected to those same announcements showing up in Google searches for him in 2009.

It is important to note that the recent CJEU order in Google Spain only required the removal of the La Vanguardia links on sub-domains (i.e., google.co.uk) and not on Google.com. The case also did not require the removal of the original announcements from La Vanguardia, but rather made those announcements harder to find. What is unclear is what would have happened had those same announcements only existed online as most of our news does now.

Google Spain dealt with accurate, albeit old, data. Some have suggested that this is akin to having a record expunged or removing something from your credit report after a pre-determined period of time and thus, should not be cause for alarm. Most would agree that there is little downside to removing information that is inaccurate or out of date. That seems rather straightforward. What is more troublesome is the idea that information determined to be “irrelevant” or “excessive” could be removed. What is even more troubling is to decide who bears the burden of deciding whether data is “irrelevant” or “excessive.”
EU GENERAL DATA PROTECTION REGULATION

Many feel that the EU Directive does not sufficiently address the internet and needs to be revised. Because of this, the European Commission proposed a General Data Protection Regulation in 2012 that will supersede the EU Directive, once it has been approved. The proposed regulation states that data subjects can request the removal of data that 1) was collected when they were a child, 2) is no longer necessary for the purpose it was collected, 3) is subject to withdrawn consent, 4) has a storage period that has expired, or 5) does not comply with some other regulation.4

Another proposal suggests that the burden of proof should be reversed, making it the data controller’s responsibility to prove that the data cannot be deleted because it is necessary or relevant.5 Article 3 of the proposed regulation affirms that non-European companies, when offering services to European customers, must apply European rules.6 The EU’s proposed regulations also call for each of the member states to pass national legislation that reconciles the revised “right to be forgotten” with the “right to freedom of expression.”7

CURRENT U.S. PROPOSALS

A Consumer Privacy Bill of Rights currently is making its way through Congress. It is a complex bill, including initiatives to protect students’ identities, national data breach notification measures, “do not track” options, and the like.8 To date, there has no draft of any “right to be forgotten” legislation issued to the public. However, the initial public comment on the 2012 draft indicates that related legislation will be proposed sometime in 2015.9

The Consumer Privacy Bill of Rights spawned proposed legislation related to the “internet of things,” particularly the types of data that are collected and reported about users of networked products.10 Networked products can include appliances, wearable technology, and the like. The legislation proposes a way for users to opt out in certain situations, but there are many challenges that remain unaddressed. The legislation begins to address issues of collection, storage, and use of this form of “personal data.” In some instances the data may be benign (e.g., your washing machine is due for service, or a particular part is malfunctioning). In some instances, the data may be problematic (e.g., your travel patterns and present location can be inferred). It is critical for all of us to engage in a national discussion about the secure collection, storage, and use of our “personal” data. This issue will only become more relevant as the volume of this data increases.

Proceeding with an approach similar to the EU Directive here in the U.S. is worrisome because private companies (data controllers) would likely be tasked with determining data “relevance, adequacy, and excessiveness” or risk being sued. This task would be costly and time consuming. For example, the day after Google posted a data removal request form on its website in response to the ruling in the Google Spain case, it received over 12,000 requests for the removal of links.11 As of this writing, Google has now processed 1.2 Million URLs and removed 42.1 percent of them.13

The removal of data upon request will likely produce a written history with “memory holes.” Shifting the burden to data controllers could also encourage meritless claims. There would be little deterrent to sending in numerous removal requests.

While we already have takedown provisions in the Digital Millennium Copyright Act (the “DMCA”), that Act deals primarily with copyright-protected information and is geared toward business interests. Importantly, the DMCA does not address the types of information that the EU Directive was designed to regulate (e.g., inaccurate, excessive, irrelevant). Recently, a court handed down the first ruling awarding damages in a false DMCA case, but many data controllers may opt to take down rather that expend time, energy, and money fighting in court.14

Some have suggested that there should at least be a mechanism to remove information we post about ourselves (e.g., poorly thought out photos, FB rants, etc.), but that would only address some of the information currently regulated by the EU Directive. For example, there are revenge sites that can create serious reputational harm for people. Currently, redress for this is costly, if it exists at all. At this time, people must approach the service provider where the offending content is displayed and request that the content be taken down. The difficulty is increased when the original post was done anonymously. In those cases, a subpoena

Fall 2015 New Hampshire Bar Journal

If society feels that access to outdated or inaccurate information is of sufficient concern that it should be removed from the reach of search engines, as opposed to requiring users to assess information found online with a critical eye, then the determination of what stays and what goes should arguably be done out in the open and with public resources.
Perhaps a free and open discourse is the best way to flush out false information. Nevertheless, the challenge for all of us is to evaluate how we judge the sources of our information. We need to acknowledge when content is sponsored, and we need to appreciate that the accuracy, relevance, and amount of information on any given topic are largely untested.

may be necessary to determine the identity of the poster. This can be a very expensive solution, and data may be removed under mere threat of lawsuit.

One of the risks of adopting an EU-like “right to be forgotten” is that the process may remove truthful information that a data subject and/or a data controller deem “irrelevant” or “excessive” resulting in patchy, biased histories. The EU Directive’s proposed legal framework could create a chilling effect and encourages censorship of “unfavorable” information.

If society feels that access to outdated or inaccurate information is of sufficient concern that it should be removed from the reach of search engines, as opposed to requiring users to assess information found online with a critical eye, then the determination of what stays and what goes should arguably be done out in the open and with public resources. Private individuals or corporations should not be given such broad power to determine which data is irrelevant, excessive, or inaccurate.

One potential benefit of an EU-like “right to be forgotten” is that individuals would have a mechanism for removing false online information about themselves. However, it is important to remember that a “right to be forgotten” is different from a “right to privacy.” The “right to privacy” is concerned with information that is not publicly known. In contrast, the “right to be forgotten” relates to removing data from the public’s knowledge (e.g., making it unsearchable).

The “right to be forgotten,” in part, allows a person to wipe the slate clean and start over. This is not a new concept. Where things get tricky is that a “right to be forgotten” also purports to remove “irrelevant” or “excessive” information. As discussed previously, the determination of what is “irrelevant” or “excessive” is subjective, at best.

One solution to the problem of “inaccurate, excessive, or in-
relevant” information that has been suggested is to give people an opportunity to “reply” to information posted about them online. Rather than remove information that people identify as inaccurate, out of date, or incomplete it would provide people with an opportunity to rectify the data. Thus, information would not be erased, but would be put in context. This option could help mitigate some of the issues relating to the erasure of information. This option could also solve issues relating to the inherent difficulties in determining what is inaccurate, excessive, or irrelevant in a particular case.

If nothing else, the Google Spain case highlights the fact that the information we find on the internet may not be accurate, relevant, or timely. When it comes to information about other people, we need to weigh the credibility and relevance of what we find online now that our entire lives are chronicled and searchable. When it comes to information about businesses and other entities, we also need to be aware that there is a concerted effort to produce what has been called “sponsored content.” These advertisements are constructed and placed to mimic the form of an original publication (e.g., a FB post, a NY Times article, etc.) but are used to raise brand awareness or to push a particular agenda. If we choose to adopt an EU-like “right to be forgotten” for individuals in the U.S., do we also need a similar process for removing speech that is equally as inaccurate, excessive, or irrelevant in a particular case.

CONCLUSION

The “right to be forgotten” may sound tempting, but it would not absolve us from being discerning consumers of information. It also would not solve all of the issues surrounding inaccurate, irrelevant, or excessive information on the internet. A “right to reply” would address some of the weaknesses of the “right to be forgotten” approach, but it is not clear if individuals would only be able to reply to information about them or if replies could come from “interested parties.” The “right to reply” will also create additional data that may be inaccurate, irrelevant, or excessive.

Perhaps the system we have now, however fallible, is best left alone. Perhaps a free and open discourse is the best way to flush out false information. Nevertheless, the challenge for all of us is to evaluate how we judge the sources of our information. We need to acknowledge when content is sponsored, and we need to appreciate that the accuracy, relevance, and amount of information on any given topic are largely untested. While a free and open conversation is not always pleasant, or easy, it does reflect our belief in the first amendment and may prove to be the best solution for us.

ENDNOTES

2 Directive No. 95/46/EC at Article 12.
3 Id.
5 Id.
6 Id.
7 Id.
13 Id.

ABOUT THE AUTHOR

Kimberly A. W. Peaslee, Ph.D., practices at Upton & Hatfield in Concord, NH. Her practice focuses on all forms of intellectual property protection, monetization, and enforcement. As a registered patent attorney, her patent prosecution practice covers a wide variety of technology areas. Peaslee’s design and brand practice utilizes design patents, trademarks, and copyright protection to provide clients with layered protection in the U.S. and around the world. Contact her at kpeaslee@uptonhatfield.com.