Euro Security Experts Deem 'Right to be Forgotten' Impossible

by Justin Brookman [1]
December 4, 2012

Just before Thanksgiving, the European Network and Security Agency (ENISA) — an agency of the European Union tasked with improving network and information security — issued an extensive analysis [2] of the controversial "Right to be Forgotten" contained in recently proposed European privacy legislation [3]. CDT has been generally supportive of the proposed Regulation (a reboot to the current, inconsistent Directive was long overdue), but we've criticized [4] some elements — such as the Right to be Forgotten — as impractical and ultimately counterproductive for consumers.

In its analysis, ENISA comes to the same conclusion that we have: that a universal Right to be Forgotten is technically impossible on an open internet. It is simply not feasible to track down and erase all copies of factual information that had previously been made public. This is a welcome development, and hopefully will serve as a reality check against magical thinking [5] that the Right to be Forgotten can easily be shoehorned onto the internet. However, as an alternative, ENISA proposes a panoply of half measures including informational Digital Rights Management and internet filtering to imperfectly simulate a Right to be Forgotten. While CDT believes strongly in the importance of developing practical policy solutions to preserve privacy on the open internet, we believe that these measures would ultimately do more harm than good. Instead, we recommend that the Right to be Forgotten be reconstituted as a more limited Right to Erase information that you've personally shared with online service providers, and that individuals be empowered to prevent the unwanted disclosure of personal information in the first place.

One Does Not Simply Eliminate Public Facts

The first part of the ENISA report lays out the practical reasons that a Right to be Forgotten can't work. You should read them for yourself, but they're many of the same intractable questions that critics have identified since the proposal first came out: who gets to decide when to erase facts that pertain to more than one person (e.g., David and Sarah got married), how to deal with individuals repurposing information in social media (Sarah retweeting something David said), and how to deal with the practicalities of redundant storage. And there's also the fundamental problem of how to a Right to be Forgotten intersects with legitimate free expression and journalistic reporting of truthful personal information.

Eventually, the report comes to the crux of the matter, concluding that a reliable Right to be Forgotten on the internet is simply not feasible: "enforcing the right to be forgotten is impossible in an open, global system, in general." This is because on the internet both readers and speakers often enjoy a degree of anonymity making the reliable and consistent identification of potential objectors and online publishers impossible. How do you contact a speaker of information if you don't know who he (or she) is? How can publishers reliably know that a complaint comes from the individuals that the asserted facts pertain to?

The only way to achieve a Right to be Forgotten would be to fundamentally rework the nature of the internet, requiring verifiable identity authentication to access and distribute information online. As such, the Right to be Forgotten would perversely represent a tremendous blow to personal privacy. Individuals would be forced to hand over personal identifying information to everyone else on the web, eliminating anonymous and pseudonymous speech online. We would lose the personal privacy that allows individuals to experiment and express themselves as they wish — not as they think others expect them to.

Fortunately, ENISA does not seem to be calling for this, but is simply identifying how the Right to be Forgotten is incompatible with the internet. However, historically we have seen calls [6] for mandating a real identity authenticated web. To date, these calls have been mostly unsuccessful (a

law requiring real name attribution in South Korea was recently struck down [7]), but preserving online anonymity is fundamentally vital to a free and open internet. A Right to be Forgotten would eliminate that.

The Right to be Mostly Forgotten?

The ENISA report wades into murkier territory when as it tries to explore other solutions that might approximate a Right to be Forgotten.

The most troublesome aspect of the report seems to endorse mandatory internet filtering as a way to ensure that disappeared information is less likely to be spread online:

One such approach relies on the observation that users typically find information on the Internet by issuing queries to a search engine, or by using a social networking, sharing, or tagging site. Data not identified by a search engine or shared via a service like Twitter is difficult to find. A natural way to "mostly forget" data is thus to prevent its appearance in the results of search engines, and to filter it from sharing services like Twitter. EU member states could require search engine operators and sharing services to filter references to forgotten data. As a result, forgotten data would be very difficult to find, even though copies may survive, for instance, outside the EU jurisdiction.

Requiring neutral intermediaries to filter potentially objectionable content is an extraordinarily dangerous idea. Setting aside for the moment the technical impossibility of scalability and filtering for all the different iterations of *a fact* (e.g., John Smith stole a car, John Smith broke the law, John Smith is a thief, John Smith reportedly stole a Ford, an image of John Smith approaching a car, a podcast discussing the allegations, etc.), governments should not be creating blacklists of information that must not be spoken. Should politicians have the power to mandate that citizens unremember inconvenient facts? Do we want to export this idea to totalitarian regimes [8] to facilitate pre-screening of what facts may be publicly uttered?

Worryingly, mandatory real-name authentication and internet filtering were also elements of the Commission's recently leaked (and much-derided [9]) Clean IT initiative to fight internet terrorist organizing. That proposal [10] too would have pushed internet intermediaries to police content against a nebulously defined set of criteria. And it too was heavily criticized [11] for substantially weakening individual privacy and free expression rights, as intermediary level platforms would be charged with monitoring and censoring user communications. Hopefully the uproar from civil society [12] that this initiative engendered will deter policymakers from trying to implement similar measures in support of a partial Right to be Forgotten.

The Right to Erase

Instead of a broad and impractical power to erase all iterations of controversial information, we've proposed instead that the Right to be Forgotten be reformulated as a more limited Right to Erase — if you choose to host or store data with a particular service provider (such as a cloud email service or a social networking site) — then you should have the right to delete that data. However, if you've previously made the decision to share information publicly, you can't reasonably expect the internet to go out and retrieve all that information for you. Nor should the Google and Facebooks of the world be responsible if someone uses their platforms to republish previously public information. Rather, if an individual has a legitimate gripe about another person violating their privacy rights on an intermediary's platform, that other person should be held responsible, and not the platform that unconsciously hosted the information. Platforms do not have the organizational or moral capacity to legally adjudicate between one member's privacy rights and another's free expression rights. Moreover, putting that kind of content monitoring obligations on intermediaries will discourage them from providing open platforms for user speech and encourage risk-averse takedowns of any speech that might prove controversial.

However, while we're skeptical of a broadly construed Right to be Forgotten, we strongly disagree with the notion that individuals don't have reasonable privacy rights and expectations in the internet age. To the contrary, we strongly agree with the ENISA report's stressing the principles of minimal disclosure and minimal duration of storage. CDT believes very strongly in technological tools to

prevent the leakage of personal information to people and companies you're not trying to communicate with, as well as legal rights to prevent secondary use and disclosure for marketing and other otherwise legitimate purposes you might not like. At the same time, privacy law cannot be construed to trample other individuals' free expression rights that are guaranteed by Article 10 of the European Convention on Human Rights, or a robust free press unfettered by government censorship. Government authority to eliminate factual information from the platforms of the internet would be a tremendous threat to those values.

Links:
[1] https://cdt.org/personnel/justin-brookman
[2] http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/the-right-to-be-forgotten
[3] http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf
[4] https://www.cdt.org/report/cdt-analysis-european-commissions-proposed-data-protection-regulation
[5] http://www.washingtonpost.com/opinions/why-we-need-to-let-our-online-memories-go/2012/11/23/29d0e54e-33ec-11e2-bfd5-e202b6d7b501_story.html
[6] http://www.hartfordinfo.org/issues/documents/FamiliesandChildren/htfd_courant_030907.asp
[7] http://online.wsj.com/article/SB10000872396390444082904577606794167615620.html
[8] https://www.cdt.org/blogs/kevin-bankston/0312stark-lesson-syria-un-must-condemn-not-condone-internet-blackouts
[9] http://www.techdirt.com/articles/20120921/03581820457/eu-officials-propose-internet-cops-patrol-no-anonymity-no-obscure-languages-because-terrorism.shtml
[10] http://www.edri.org/files/cleanIT_sept2012.pdf
[11] http://www.edri.org/cleanIT
[12] https://www.accessnow.org/blog/100512-access-comments-on-commission-consultation-on-self-regulation/