

European Commission Proposes Stronger Data Privacy Legislation

by [Justin Brookman](#) [1]

February 2, 2012

After weeks of suspense and rumors, last Wednesday the European Commission finally introduced [long-awaited legislation](#) [2] to update the 1995 Data Protection Directive, the primary instrument governing personal privacy in Europe. These changes had been widely anticipated by the privacy community, and were spurred in large part by two distinct motivations: (1) the desire to provide users stronger rights over their personal information, and (2) a wish to harmonize divergent privacy laws across all the European Union.

Ironically, the same goals drove the passage of the first EU Data Protection Directive 17 years ago. At that time, there were few comprehensive privacy laws in Europe (or anywhere else, for that matter). The initial Directive required member states to pass enacting legislation codifying the principles contained within the document, whilst allowing for a margin of interpretation that would prove its limits in practice. In the intervening years, the EU's 27 member states have all implemented and interpreted the Directive in varying ways, leading to a fair amount of confusion for companies offering services across the internal market. And while each country is slightly different, enforcement has been consistently spotty across the continent, leaving users with the suspicion that their information is not adequately protected as companies utilize increasingly sophisticated technologies to track user behavior.

The Commission has been working on the text of the legislation for over a year and has been consulting stakeholders for more than two years; in December, what was purportedly a [near-final version](#) [3] was widely leaked and analyzed. The most significant change in that draft was that the legislation was in the form of a regulation instead of a directive, meaning that it would be automatically binding on member states (rather than a mere instruction to national governments to pass consistent legislation). The draft contained other provisions designed to make complying with European privacy law simpler for companies — such as subjecting companies to the jurisdiction of one lead national data protection regulator, rather than 27 potentially different authorities. The draft legislation also eliminated the burdensome and often costly requirement that companies provide regulators with pro forma (and typically ignored) notification in advance of all data processing activity (and paying filing fees for the privilege).

The legislation provided new protections for users, such as a strict data breach notification standard, a requirement that all consent to collect and use personal data be upfront and explicit, and a “right to be forgotten” — the ability of users to erase (at least some of the) information held about them by others (to some extent, the “right to be forgotten” is to the Commission proposal what “Do Not Track” was to the [December 2010 FTC privacy report](#) [4] — a small section that received outside media coverage and attention from stakeholders). It also called for stronger powers for regulators, including expanded jurisdiction and the ability to obtain fines as high as 5% of global revenues for privacy violations (for a large international company, this could easily run to the hundreds of millions of dollars, though the legislation does include language that the penalty must be “proportional” to the scope of the violation). In response, many (especially in the United States) criticized the heightened user protections as being unworkable and unduly burdensome on industry; the United States Department of Commerce reportedly [lobbied extensively](#) [5] to have the legislation revised prior to formal introduction.

Good Faith Effort

The version released by the Commission last week does address many of the criticisms that had been leveled, and appears to be a good faith effort to find middle ground between user's rights, practical implementation and the costs imposed on businesses. For example, the compromises include a less prescriptive data breach rule and a 60% decrease in the maximum penalties a

regulator can levy. The legislation still has its critics from both [civil society](#) [6], [industry](#) [7], and member state [Data Protection authorities](#) [8], and there will be intense lobbying as the bill is debated and amended in the European Parliament and Council over the next two years (at least). CDT supports the aims of the proposed legislation, but there remain significant issues that need to be addressed in the current text. We will be putting out more detailed analysis of the particulars of the bill — along with suggested amendments — in the weeks to come.

(A side note to all this is that many online privacy issues may not be much affected by this new law. In 2002, the European Union passed a [specific law on e-Privacy](#) [9] that governs issues like cookies and online behavioral tracking. Of course, the Data Protection Regulation could be revised to specifically supersede the e-Privacy Directive if officials believe the Regulation is sufficiently robust to address the areas the Directive was written to address. For example, Vice-President Neelie Kroes, Commissioner for Europe’s Digital Agenda, [has endorsed](#) [10] “Do Not Track” as a possible global solution to clear up the substantial uncertainty around the e-Privacy Directive and potential conflicts among European --and other-- laws governing online tracking.)

Although the particulars are still being worked out, the legislative proposal makes significant progress on the Commission’s primary focus of giving users strong, consistent protections across the Union. It represents a frank admission that the strong principles contained in the 1995 Data Protection Directive haven’t been implemented in a consistent and effective manner in practice to protect users, and that more rigorous laws are needed. If successful, the new regulation will better secure user data while offering companies a clear, predictable path to regulatory compliance; at worst, this same scenario could be playing out in another 20 years, as another Commission tries to find a new legal means to protect personal information across Europe.

-
- [Data Protection Directive](#)
- [consumer privacy: EU](#)

Copyright © 2013 by Center for Democracy & Technology. CDT can be freely copied and used as long as you make no substantive changes and clearly give us credit. [Details](#).

Source URL:

<https://www.cdt.org/blogs/justin-brookman/22european-commission-proposes-stronger-data-privacy-legislation>

Links:

- [1] <https://www.cdt.org/personnel/justin-brookman>
- [2] http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm
- [3] <http://amberhawk.typepad.com/amberhawk/2011/12/draft-data-protection-regulation-leaked-doubtful-whether-it-will-get-enacted-in-this-form.html>
- [4] <http://www.ftc.gov/os/2010/12/101201privacyreport.pdf>
- [5] <http://www.edri.org/US-DPR>
- [6] <http://www.edri.org/CommentsDPR>
- [7] <http://www.reuters.com/article/2012/01/24/us-europe-data-legislation-idUSTRE80M1VL20120124>
- [8] <http://www.huntonprivacypblog.com/2012/02/articles/german-dpas-comment-on-proposed-eu-data-protection-law-reform>
- [9] http://europa.eu/legislation_summaries/information_society/legislative_framework/l24120_en.htm
- [10] <http://blogs.ec.europa.eu/neelie-kroes/donottrack/>