

# GDPR Should Have Made Cookies Toast



BY **MARK DIXON**

On Friday, Europe will see a new law come into force: the hard-to-understand General Data Protection Regulation (GDPR).

Its goal is to tip the balance back in favor of citizens and away from data-abusing companies by regulating what companies can do with people's data. It's supposed to give people control by requiring disclosure of how their data will be used and by forcing companies to get permission in advance—to get users to press the so-called 'opt-in' buttons.

It's also going to cost European and global companies a lot of money to comply, estimated at \$100 billion prior to the deadline and tens of billions of dollars per year going forward for IT and new staff, such as data protection officers. Companies are frustrated by the cost and vagueness and are scrambling to meet Friday's deadline.

The problem is that the pain the rules inflict on companies isn't nearly matched by the protection it will give to users. Legislation is never popular with everyone, but it should

bring more benefit than hardship. This is an example of a piece of legislation that was well intentioned but won't work.

Yes, ensuring people's data isn't collected, stored, or used without their permission sounds all well and good. But the crux of the issue is not whether you give permission, but whether you can, in practice, make the right permission decision. What's the value if you can't easily understand what exact permissions you're giving and what they're being used for?

The only change the regulation will bring is getting users to opt-in who in practice don't know what they are opting into.

This is because the regulation allows the details of what you're signing up to to be buried in the fine print of the privacy policy, and it doesn't require disclosure of exactly how the different permissions will then be used to manipulate you online. And once you've given permission, it does nothing to force companies to inform you while you're being tracked.

What is needed is a regulation that is strong enough to really give people practical control of their data. After all, it is our data, isn't it?

## Target the cookie

The real battleground should be the cookie.

The regulation does little to change the way cookies monitor us on a site. You'll be tracked and manipulated just like before. Your right to withdraw your permission or have your data deleted does exist under the regulation but, with the burden of effort on you to initiate this, it will be 'manipulation as usual.'

The well-intentioned regulation is made impotent by its conceptual flaw that if something is obtained legally, then that makes it okay by definition, and that if people don't read or can't understand the consequences of the privacy policies, that's their problem.

## We are all human beings

The rules ignore that we are human beings. How many people won't accept the cookie? How many have the time not to? And if—in a blue moon of unlikelihood you do anything other than just say yes to get rid of that mosquito in front of your face—you will then only

find yourself immersed in the legalese of what opting in means, where your chance of understanding it is the square root of zero—even if you're a lawyer.

The reason this is important is that permission is being obtained in an underhand way—in effect being tricked out of us. On top of that, you'll often have no idea of the consequences of refusing—whether it means you'll lose useful functionality or will benefit from not being monitored. This lack of clarity of the consequences pressures you into opting in.

## Make cookies honest or toast

Simple-to-understand transparency is needed to make clear what will happen if you opt-in or opt-out.

This information should be presented in a standardized way and shown simultaneously with the request for permission so users become familiar with the layout and easily take the permission trade-off decision.

The permission window should show an 'Honesty in Tracking' or 'Honesty in Data' checklist such as this:

### ***If you opt-in, we will:***

- track your navigation to influence which ads or products you'll see
- use your data to change the prices we offer you
- make use of data we obtain from third parties about you or your behavior
- sell or release data about you to third parties

### ***If you opt-out, you will:***

- be able to use the site's functions unaffected
- have access to fewer or weaker functions
- see generic ads rather than ones customized based on what we know about you

or

- be blocked from use of the site

This disclosure is the only way for cookies to protect the user. Cookies as we know them should be toast.

## Track the tracking

And there's another key shortcoming of GDPR. While it provides the right to have your data deleted, it omits the equally important right to be kept aware of what's being done with you after you give permission.

The solution is that whenever a site is tracking you through your IP address or otherwise, it should be required to display a standard icon—perhaps a bright red eye—to indicate you're being watched. This way at least you can track you're being tracked. This 'tracking eye alert' should also act as a click-through to open the same standardized 'Honesty in Tracking' window and let you withdraw permission in the same screen.

## America's chance

By not requiring transparency and standardization in cookies and not forcing sites to display ongoing tracking, GDPR is losing a huge opportunity to protect our online data privacy.

Cookies, as they will exist after the regulation, deserve the equivalent of a government health warning. Just like mass-produced edible cookies, online ones shouldn't be sold without proper packaging. People need to know the ingredients—the consequences of swallowing them—on the label in plain English.

Human beings will never read 20-page privacy policies, so there will be little benefit from GDPR in practice. Meanwhile, \$100 billion is a lot of money. GDPR is thus a very bad return on investment.

Europe has taken the lead but has gotten it wrong. When America finally wakes up to the need for online data protection, it will have the chance to learn from the mistakes of Europe and go for something radical, in the spirit of an amendment to the Constitution, which truly gives the people's data back to the people.

*Mark Dixon founded and runs boutique mergers and acquisitions advisory firm [the1.com](#) and was a co-founder of [BreakingViews.com](#).*

### FORTUNE



40 Under 40	Home	Health	Technology	Fortune Knowledge Group	About Us
100 Best Companies to Work For	Automotive	International	The Ledger	Fortune Data Store	Subscribe
Fortune 500	Careers	Leadership	Venture	Fortune Conferences	Give a Gift
Global 500	Design	Luxury	Photography	Customer Service	Ad Choices
Most Powerful Women in Business	Energy & Environment	Markets	Podcasts	EU Customer Service	Terms of Use
World's 50 Greatest Leaders	Executive Travel	Most Powerful Women	Videos	Site Map	Your California Privacy Rights
World's Most Admired Companies	Finance	Retail	Newsletters	Privacy Policy	
All Rankings	Commentary	Sports	Magazine	Advertising	

© 2018 Time Inc. All Rights Reserved. Use of this site constitutes acceptance of our [Terms of Use and Privacy Policy](#) (Your California Privacy Rights).

Fortune may receive compensation for some links to products and services on this website. Offers may be subject to change without notice.

Quotes delayed at least 15 minutes. Market data provided by [Interactive Data](#), ETR and Mutual Fund data provided by [Morningstar](#), Inc. Dow Jones Terms & Conditions: <http://www.djindexes.com/imd/46000.html?topic=infocenter&index=1000>.

S&P: Index data is the property of Chicago Mercantile Exchange Inc. and its licensors. All rights reserved. [Terms & Conditions](#). Powered and implemented by [Interactive Data Managed Solutions](#). | EU Data Subject Requests