

How Silicon Valley gamed Europe's privacy rules

The region's data protection overhaul was supposed to help citizens. Instead, it's helped Big Tech.

By **MARK SCOTT, LAURENS CERULUS AND STEVEN OVERLY** | 5/22/19, 10:40 AM CET | Updated 5/26/19, 7:50 PM CET



It's arguable that Europe's privacy rules merely build on what has been on the legislative books for decades | Image via iStock

When Europe's tough privacy rules came into force on May 25, 2018, policymakers and industry executives expected a series of dominoes would soon start to fall.

Global technology giants like Facebook would feel the heat of fines of up to 4 percent of their total yearly revenue. Companies like Google would think twice before pushing ahead with aggressive new ways of collecting people's data. Smaller rivals would be given greater space to

compete.

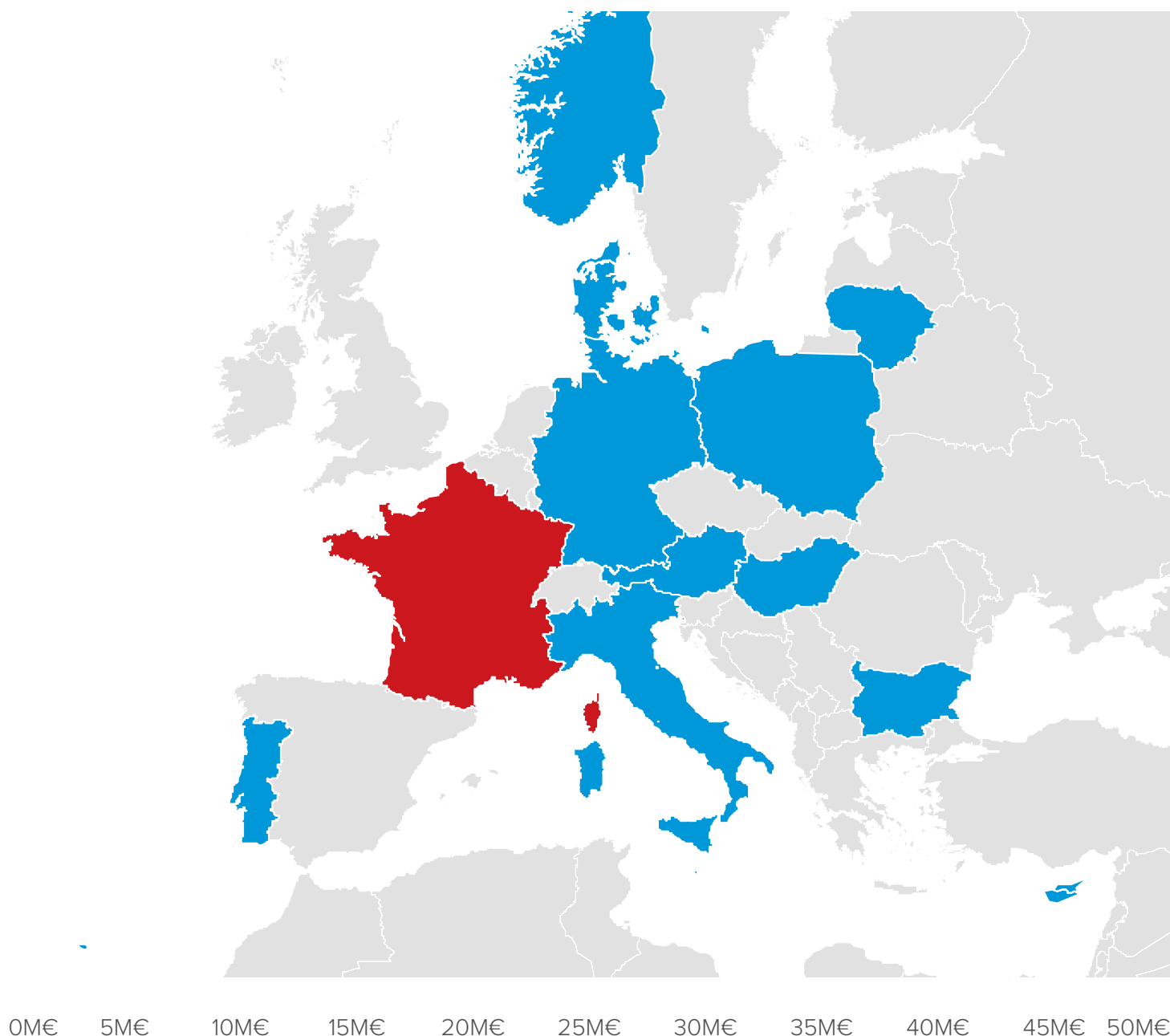
But a year later, none of those dominoes have yet fallen, according to interviews with senior policymakers, tech executives and privacy campaigners.

Big fines and sweeping enforcement actions have been largely absent, as under-resourced European regulators struggle to define their mission — and take time to build investigations that will likely end up in court.

New forms of data collection, including Facebook's reintroduction of its facial recognition technology in Europe and Google's efforts to harvest information on third-party websites, have been given new leases on life under Europe's General Data Protection Regulation, or GDPR.

GDPR IN NUMBERS

A year after it came into force, Europe's new privacy rules have only triggered one major fine.



SOURCE: enforcementtracker.com

POLITICO

Smaller firms — whose fortunes were of special concern to the framers of the region's privacy revamp — also have suffered from the relatively high compliance costs and the perception, at least among some investors, that they can't compete with Silicon Valley's biggest names.

"Big companies like Facebook are 10 steps ahead of everyone else, and 100 steps ahead of regulators," declared Paul-Olivier Dehaye, a privacy expert who helped uncover Facebook's

Cambridge Analytica scandal. “There are very big questions about what they’re doing.”

The patchy record of Europe’s data protection overhaul — on the one-year anniversary of its implementation — has given industry an opportunity to blunt similar efforts outside the European Union to emulate the region’s new privacy rules.



ALSO ON POLITICO

New US privacy oversight on the table for Facebook, Zuckerberg

NANCY SCOLA



ALSO ON POLITICO

How lobbyists rewrote Washington state’s privacy law

MARK SCOTT

Campaigners and some lawmakers from Colombia to South Africa and even the United States clamor to import similar protections, claiming that only strict restrictions will grant citizens sufficient control over their data.

But aggressive industry lobbying in capitals worldwide has worked hard to frame Europe’s laws as overly cumbersome, particularly for small companies, with technology groups warning other politicians not to merely copy Europe in the rejiggering of their own local privacy standards.

“A lot of small and medium-sized businesses are still struggling,” said John Miller, vice president of policy at the Information Technology Industry Council, a trade group in Washington, D.C. that represents many of Silicon Valley’s biggest names. “How do we protect the rights of consumers here without making the law quite so onerous?”

GDPR, one year on

It was not supposed to be this way.

When Europe unveiled its privacy revamp, European officials hailed it as a major victory for consumers — a message that piggybacked on the public’s growing awareness of their data rights after Facebook’s Cambridge Analytica scandal, in which roughly 87 million of its users worldwide had their data misused during political campaigns.

Policymakers like Andrea Jelinek, an Austrian official in charge of a pan-regional group of EU data protection regulators, gave evidence to the U.S. Congress on how Europe has implemented its new laws. Mark Zuckerberg, Facebook’s chief executive, promised to offer European-style protections to all of his company’s 2.2 billion global users.

But since the region’s standards came into force a year ago, few companies have yet to have their wings clipped by the new regulation — and some of the world’s largest tech companies have used their significant in-house regulatory and financial muscle to turn Europe’s privacy push to

their advantage.



"There has been a dramatic change both in the attitudes toward the tech firms and, I would say, in the views of European privacy law"

— *Marc Rotenberg, executive director of the Electronic Privacy Information Center*

So far, almost 100,000 privacy complaints have been filed with national privacy regulators, though only a few have led to meaningful penalties, according to the International Association of Privacy Professionals, an industry trade body. Total fines have now reached roughly €56 million, although almost all of that came from a one-off €50 million levy against Google by French officials (the search giant is appealing that decision).

National agencies — often small, obscure regulatory offshoots that lack the manpower or legal resources to keep large multinationals at bay — have struggled to give Europe's privacy rules real bite, despite widespread government efforts to increase their yearly budgets. Officials urge restraint, saying that it will take time for the full force of Europe's privacy rules to take effect and that companies are already changing how they collect people's data because of potential blockbuster fines.

"Even after 12 months, the reality is that there is no consensus or clear harmonization for how data should be processed," said Ahmed Baladi, co-chair of the privacy, cybersecurity and consumer protection unit at Gibson Dunn, a law firm in Paris. "We still need more guidance from national authorities."

Facebook and Google

Into this void has stepped Big Tech.

Ahead of Europe's privacy overhaul, Facebook spent months preparing to restart its facial recognition service in the region — technology that the company believes now meets the region's beefed-up standards. Ireland's data protection agency, which oversees the social media giant's activities in the EU, has yet to take a position on the matter.

Despite the previous ban, Facebook's facial recognition technology is now permitted in Europe because users are actively given the choice to opt into the service. The social networking giant also restarted the sharing of some data between WhatsApp, its popular messaging service, and Facebook — a practice that had similarly been outlawed in some states in the 28-country bloc.



A Facebook logo on a stand during the VivaTech startups and innovation fair, in Paris, France, May 16, 2019. | Julien de Rosa/EPA-EFE

Even now, some privacy regulators aren't convinced that people understand how their data may be used and that others could still have their digital information collected without consent. Facebook denies it stores data on individuals who have not chosen to use its facial recognition technology.

"Processing of biometric data such as in automatic facial recognition comes with substantial risks," Johannes Caspar, head of the Hamburg privacy regulator, said in an email. "Facial recognition must be strictly limited to those users who have opted in to that technology."

Google also moved quickly to cement its position in the data economy.

Weeks before Europe's new rules became law, the search giant contacted all websites, both inside the EU and elsewhere, that relied on the company's dominant advertising services, informing these publishers that they would now have to solicit people's consent to collect data on Google's behalf.

Under Europe's new privacy standards, the tech giant must get people's permission to target them with digital advertising. But by forcing publishers to do this work for Google — the search giant said if websites did not comply, they would not be able to use the company's advertising services — it added an additional line to the company's revamped privacy settings, which allowed Google to take ownership of people's data from publishers that it then could use for its

own undefined purposes.

In response, the tech giant said these changes were necessary under Europe's new data protection rules, and that it had not taken greater control over data collected by publishers worldwide.

Yet in a sign of potential future privacy woes for Google, an investigation into the legality of such practices is expected to be announced in the coming weeks, according to an industry executive with knowledge of the matter.

For Jason Kint, chief executive of Digital Content Next, a trade body for publishers including the New York Times and the Guardian (Axel Springer, which co-owns the European edition of POLITICO, is also a member), Google's request represents a land grab for lucrative data that websites routinely have collected on their users — a crucial resource for newspapers increasingly going digital in search of much-needed revenues.

"It forced our members to give Google secondary use of their data," said Kint. "They're supposed to be transparent about what they're using the data for, but we don't really know."

First Europe, now the world

The first shots in the global privacy war were fired in Europe. But as policymakers from New Delhi to Brasilia turn their attention to reining in Big Tech's use of data, the EU's standards are now at the center of cut-throat lobbying worldwide.

That's particularly true in the United States, where lawmakers and tech executives agree on the need for new privacy rules after years of Silicon Valley's dismissal of such protections.

In recent months, Congress has held multiple hearings on privacy, and politicians are engaged in negotiations over a wide-ranging data protection bill. But Republicans and Democrats are still divided on key principles, including if a federal law should override existing state-based rules and if individual consumers should have the right to sue tech firms over privacy violations.

“GDPR is the global standard, but the history of deployment of technology in the United States is more aligned to the 'opt out' approach" — *Reuven Carlyle, a Washington State senator*

Those sticking points may threaten to derail the push for national legislation — but the fact talks are happening after years of disinterest can be attributed, in part, to the global influence of Europe's privacy rules.

"There has been a dramatic change both in the attitudes toward the tech firms and, I would say, in the views of European privacy law," said Marc Rotenberg, executive director of the Electronic Privacy Information Center, a campaigning group in Washington, D.C. "Lawmakers are genuinely asking whether the U.S. needs a law similar to Europe."

With negotiations in Washington stalled, particularly ahead of the U.S. presidential election in 2020, attention has shifted toward U.S. states, many of which are mulling wide-ranging privacy legislation that often mirrors sections of Europe's rules.

In California, which became the first U.S. state to pass wide-ranging data privacy legislation last year, lobbyists have until 2020 to soften the proposals' impact on the likes of Google and Facebook by adding industry-friendly provisions to exempt certain kinds of data collection. Companies also successfully petitioned the state's attorney general to remove the right for citizens to directly sue firms for illegally collecting their digital information.

In Washington State, local lawmakers went a step further by specifically name-checking Europe's privacy standards in proposals that narrowly failed to pass the local legislature in late April.

But whereas in Europe, people are automatically given the right to not have their information collected unless they give explicit consent to companies, the U.S. proposals, by default, had given businesses the right to harvest such data without needing to seek users' permission. That raised concerns among privacy groups that U.S. lawmakers were co-opting Europe's privacy reboot without offering the same fundamental rights to U.S. citizens — criticisms that the bill's backers deny.

"GDPR is the global standard," said Reuven Carlyle, a Washington State senator who co-sponsored the recent privacy legislation. "But the history of deployment of technology in the United States is more aligned to the 'opt out' approach. Without that, you fundamentally alter the value proposition of innovation."

CORRECTION: This story has been corrected to show that Ireland's Data Protection Commission has not yet taken a position on Facebook's facial recognition tool.