SSBG IT Solutions

Ph: (8621) 5404-3999 Fax: (8621) 5404-7759
Email: Sales1@SSBG.com.cn www.SSBG.com.cn

EUROPE'S NEW PRIVACY LAW WILL CHANGE THE WEB, AND MORE

CONSUMERS HAVE LONG wondered just what Google and Facebook know about them, and who else can access their personal data. But internet giants have little incentive to give straight answers — even to simple questions like, “Why am I being shown this ad?”

On May 25, however, the power balance will shift towards consumers, thanks to a European privacy law that restricts how personal data is collected and handled. The rule, called General Data Protection Regulation or GDPR, focuses on ensuring that users know, understand, and consent to the data collected about them. Under GDPR, pages of fine print won’t suffice. Neither will forcing users to click yes in order to sign up.

Instead, companies must be clear and concise about their collection and use of personal data like full name, home address, location data, IP address, or the identifier that tracks web and app use on smartphones. Companies have to spell out why the data is being collected and whether it will be used to create profiles of people’s actions and habits. Moreover, consumers will gain the right to access data companies store about them, the right to correct inaccurate information, and the right to limit the use of decisions made by algorithms, among others.

The law protects individuals in the 28 member countries of the European Union, even if the data is processed elsewhere. That means GDPR will apply to publishers like WIRED; banks; universities; much of the Fortune 500; the alphabet soup of ad-tech companies that track you across the web, devices, and apps; and Silicon Valley tech giants.

As an example of the law’s reach, the European Commission, the EU’s legislative arm, says on its website that a social network will have to comply with a user request to delete photos the user posted as a minor — and inform search engines and other websites that used the photos that the images should be removed. The commission also says a car-sharing service may request a user’s name, address, credit card number, and potentially whether the person has a disability, but can’t require a user to share their race. (Under GDPR, stricter conditions apply to collecting “sensitive data,” such as race, religion, political affiliation, and sexual orientation.)

GDPR has already spurred, or contributed to, changes in data-collection and -handling practices. In June, Google announced that it would stop mining emails in Gmail to personalize ads. (The company says that was unrelated to GDPR and done in order to harmonize the consumer and business versions of Gmail.) In September, Google revamped its privacy dashboard, first launched in 2009, to be more user-friendly. In January, Facebook announced its own privacy dashboard, which has yet to launch. Though the law applies only in Europe, the companies are making changes globally, because it’s simpler than creating different systems.

The law’s impact will extend well past the web giants. In March, Drawbridge, an ad-tech company that tracks users across devices, said it would wind down its advertising business in the EU because it’s unclear how the digital ad industry would ensure consumer consent. Acxiom, a data broker that provides information on more than 700 million people culled from voter records, purchasing behavior, vehicle registration, and other sources, is revising its online portals in the US and Europe where consumers can see what information Acxiom has about them. GDPR “will set the tone for data protection around the world for the next 10 years,” says Sheila Colclasure, Acxiom’s chief data ethics officer.

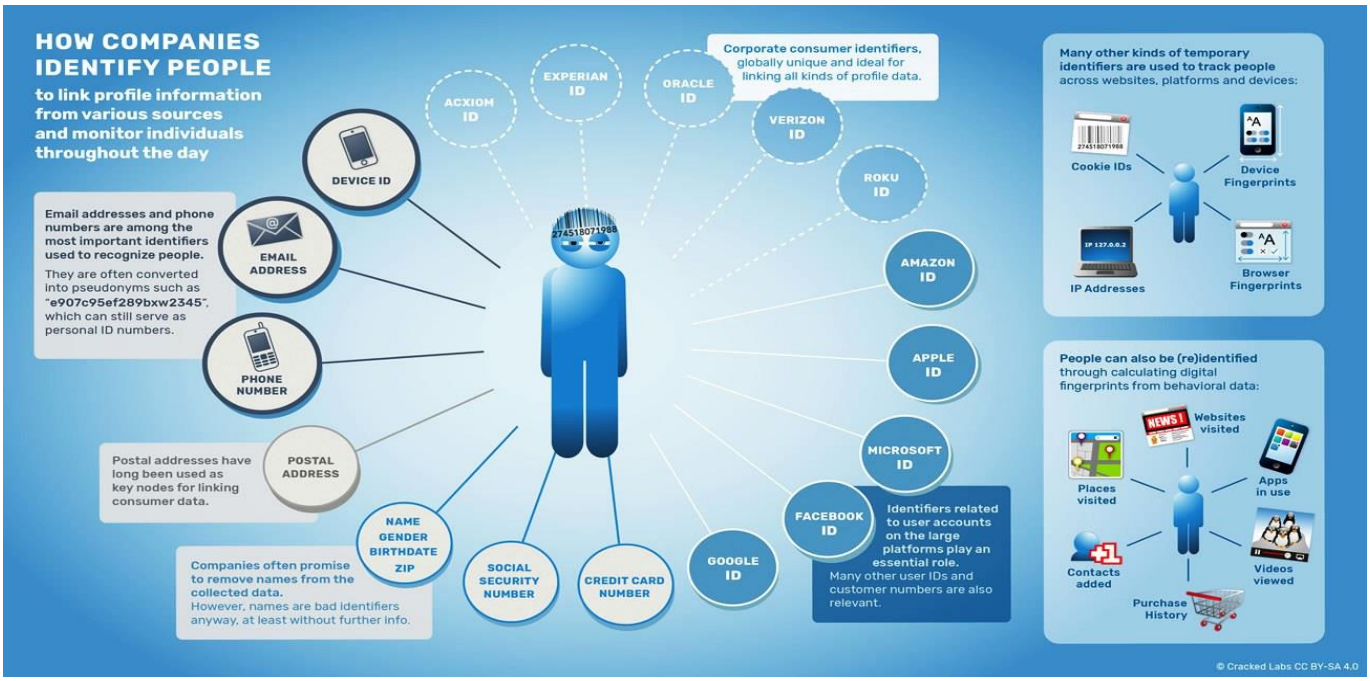
Beyond such moves, the law's emphasis on consent, control, and clear explanations could prompt users to better understand and reconsider the ways they are surveilled online. Meanwhile, privacy activists plan to use GDPR as a weapon to force changes in corporate data-handling practices.

https://twitter.com/profcarroll/status/974849812830048256

In short, the law is a chance to flip the economics of the industry. Since the dawn of the commercial web, companies have been financially incentivized to hoover up data and monetize later. Now, EU consumers will have the freedom to opt in, rather than the burden of opting out. That emphasis on consent creates a financial reward to building consumer trust.

GDPR presents "a real chance to renegotiate the terms of engagement between people, their data, and the company," rather than mindlessly clicking away a terms-of-service agreement, says David Carroll, associate professor of media design at The New School. Carroll says data collected by activists "might be the basis for new investigations and ways to keep the companies accountable."

The need for transparency and accountability is more vital than ever. Clicking to accept an impenetrable terms-of-service document once seemed like a no-brainer. The upside was incredible efficiency and the downside, it seemed, was just some annoying shoe ads stalking you around the web. But the past year has shown how the same personal data has been weaponized to suppress minority voters, radicalize young white men, exploit political beliefs to sow division, and possibly swing elections. In a white paper called "Corporate Surveillance in Everyday Life," researcher Wolfie Christl diagrams how personal data is used to influence behavior and determine what products you see, what services you have access to, and what prices you pay in areas from shopping to banking. "Every time we click, these companies are trying to figure out, is this a valuable person or this is a worthless person?" Christl says.



Researcher Wolfie Christl shows the sources of information companies tap to assemble profiles of people.

PASCALE OSTERWALDER/CRACKED LABS

Most of the data rights enshrined under GDPR were already established in the EU, but went unenforced. GDPR standardizes data rights across all EU countries, empowering regulators with the same big stick and sharper teeth. Violators face fines of up to 4 percent of annual global revenue. For Facebook, that would be $1.6 billion; for Google, $4.4 billion.

Ph: (8621) 5404-3999 Fax: (8621) 5404-7759
Email: Sales1@SSBG.com.cn www.SSBG.com.cn

Of course, the law has its share of detractors, who dismiss GDPR as more protectionism from the EU, which has challenged American tech platforms on antitrust and privacy grounds with expensive consequences. Then there are concerns about cost. Colclasure from Acxiom calls the data industry the backbone of "free content and free knowledge" online. "It's either hit a pay wall or these sites are ad-supported for the most part," she says.

There are potential loopholes in the law. It allows businesses to process personal data without consent for limited reasons, including a business's "legitimate interests," which the European Commission says includes "direct marketing," through mail, email, or online ads.
However, even then companies must take into account a consumer's expectation of how their data will be used and can't infringe on the other consumer rights guaranteed under GDPR. In the digital realm, EU consumers also have the added protection of a companion set of rules, called the ePrivacy Directive, that govern electronic communication. Under those rules, which are in the process of being ratified into law, consent is the only legal basis for collecting personal data.

David Martin, senior legal officer at the European Consumer Organisation, an umbrella group of 43 consumer groups, says tech company lobbyists are working to influence the guidelines to interpret GDPR and weaken the ePrivacy language.

Avoidance isn't an option. In 2017, Facebook's revenue per user in Europe grew 41 percent from a year earlier, to $8.86. The rate of increase was faster than any other region.
In a statement to WIRED, Rob Sherman, Facebook's deputy chief privacy officer, said, "Everyone on Facebook will see improvements to their tools and privacy controls this year. In addition to GDPR, we're looking at things across the board to see how we can give people more control and do more to help them understand how their data is used." Google directed WIRED to a 2017 blog post where the company saidit "is committed to complying with the GDPR across all of the services that we provide in Europe," including Google search, Gmail, and all of its advertising and measurement services.
Privacy activists believe the law will unlock the data they need to force other changes. It's worked before. A lawsuit filed against Facebook in 2013 by Austrian lawyer and privacy activist Max Schrems led to a ruling striking down a "Safe Harbor" agreement that companies used to transfer data between the US and Europe. Schrems' case is pending.
Emboldened by the approach of GDPR, Schrems in November launched a nonprofit called None of Your Business that will use GDPR to "confront tech giants like Facebook, Google & Co. with a team of highly qualified and motivated lawyers and IT experts on equal footing," the group said in a statement.

Paul-Olivier Dehaye, a mathematician and cofounder of PersonalData.IO, has used UK data protection law to help individuals access personal information processed by Cambridge Analytica, the controversial firm behind the data breach affecting more than 50 million Facebook users. Dehaye believes that GDPR could help pry out more information.
GDPR's ultimate impact will rest on how aggressively consumers wield their new rights. Recent trends indicate a growing interest in privacy. The use of ad-blockers and VPNs is on the rise in the US and elsewhere. Corporations have responded to the demand. In August, Mozilla introduced Firefox Focus, a private mobile browser. In September, Apple added tracking prevention to its Safari browser.
Fatemeh Khatibloo, a principal analyst at Forrester, thinks the end result will be more progressive data-collection practices. Consumers would be shocked to know the number of cookies, trackers, and ad servers firing on the web pages they visit, she says.
In a survey of UK consumers Khatibloo conducted in August, 51 percent of respondents said they were at least somewhat likely to exercise their new rights under GDPR. The most common example cited was data deletion. "People felt they could 'punish' the companies that were invasive or aggressive by asking them to delete their information," she says.

Still, Khatibloo is skeptical that GDPR will spook users of popular internet services. Consumers understand the value of exchanging their data for free services and don't want their online experience interrupted, she says.

Ph: (8621) 5404-3999 Fax: (8621) 5404-7759
Email: Sales1@SSBG.com.cn www.SSBG.com.cn

GDPR “sheds very bright light on some of the data machination that people aren’t aware of, but I don’t think that there’s going to be a huge Facebook reckoning.”

Much may turn on how companies ask for consent. In September, PageFair, which helps publishers deal with ad blockers, conducted a survey in which it presented users with choices for being tracked, such as “only accept first party tracking” or “reject tracking unless it’s strictly necessary for the services requested.” Of the 300 people surveyed, only about 5 percent consented to all tracking.
Marketing firm Criteo is aiming for something much less intrusive. In January, Digiday published a sample consent interface that Criteo was testing. It featured a tiny banner pop-up at the bottom of a page that told users that by clicking on any link on the page, they consented to Criteo’s “user-friendly, cross-site tracking technology.”
https://twitter.com/profcarroll/status/951476582190927873

Rewriting the Rules

- GDPR is prompting changes in the web's Whois directory, which may be closed to public view.
- Facebook offered advertisers the opportunity to target users as young as 14 during moments of psychological vulnerability,
- Read WIRED's coverage of the approval of GDPR in 2016.

Source: https://www.wired.com/story/europes-new-privacy-law-will-change-the-web-and-more/