Ignore Mark Zuckerberg

His promise that new EU data privacy guidelines will be "rolled out" to American users is misleading.

By **Michael Veale**, University College London (m.veale@ucl.ac.uk, @mikarv)
First published in **Slate Future Tense**, April 12 2018.

"We believe that everyone around the world deserves good privacy controls," Mark Zuckerberg told the House Energy and Commerce Committee on Wednesday. "We've had a lot of these controls in place for years. The [EU General Data Protection Regulation] requires us to do a few more things, and we're going to extend that to the world."

Until recently, U.S. discourse largely claimed new EU privacy rules were more about European protectionism than data protection. But in the aftermath of the Cambridge Analytica scandal, the idea of a U.S. data protection law is suddenly appealing to many American legislators. Zuckerberg said repeatedly before the House as well as the Senate that he is open to regulation, but he also seemed to suggest that, thanks to Facebook's embrace of the new European law, it was almost unnecessary. He promised that Facebook will ensure that "all the same controls will be available around the world." Such a pledge sounds appealing, particularly given the fact that much of Congress has a self-regulatory soft spot. But what it actually means is neither straightforward nor as protective as it may sound.

The controls he was referring to are part of Facebook's implementation of the EU General Data Protection Regulation—GDPR for short. The bloc's refreshed rules on privacy and user control of personal data will become enforceable from May 25. Fearing headlines of fines of 4 percent of global turnover in the preceding year or 20 million euros (about $24 million), whichever is higher, firms the world over are scrambling to get their houses in order. All organizations that are either based in the EU or process personal data relating to EU residents, including U.S. firms, must narrowly define and properly communicate what they want to do with the data and ensure they have a lawful basis for doing it. The regulation spells out rules for explicit consent, which can't be bundled up with other terms and conditions, when sensitive data is collected and inferred, and it has to be as easy to withdraw permission as it was to grant. Companies must also swiftly comply with requests to obtain copies of personal data, to object to particular uses of it, or to have it erased ("forgotten").

When it comes to Zuckerberg's claim, the core thing to understand is the distinction between two types of Facebook user: the 239 million located in the U.S. and Canada, served out of Facebook in Menlo Park, California, and the 1.89 billion located elsewhere and served from Facebook Ireland. The 89 percent of users served from Facebook Ireland—even those who don't live in EU countries—will already benefit from the GDPR's legal protection, regardless of public promises, and can seek redress through European regulators and courts.

Zuckerberg may want you to think that Facebook has decided to bring the remaining 11 percent up to parity. But that's not what's going to happen. Whenever asked to confirm whether Facebook would extend GDPR *protections* to the few locations they are not legally required, Zuckerberg was careful to respond that yes, they would extend GDPR "*controls*." The difference is critical. Facebook's chosen "controls" are not the same as the GDPR. Instead, they are a highly restrictive interpretation of data protection law that does not reflect the depth of transparency, accountability, and control the regulation demands.
Take the GDPR's right of access to personal data. Zuckerberg claimed to the House that everything users "have in Facebook" is available to download. Yet Facebook itself admits that this is untrue. Facebook Pixel code chunks, which make your browser reveal your identity on non-Facebook pages, are strewn across 30 percent of the web, and the company can also track users across smartphone apps. That information is stored in a nonanonymized format alongside user IDs in Facebook's "Hive" big data analysis system. Even trivial examination of such data can reveal intensely private and intimate information on individuals' characteristics, lifestyle, and preferences. And this is an organization capable of far more than trivial analysis. This year, Swiss mathematician Paul-Olivier Dehaye submitted a written request to Facebook for data about the websites he had visited and what had been inferred about him. In response, the company said that while it could retrieve the information, pulling it out of the many parts of the complex Hive analysis system it had been placed across would "entail multiple hours of total computing time, across thousands of servers running in parallel." If Facebook offered everyone the ability to understand and control this data, it claimed, the "required computer processing power would greatly exceed that available to the Facebook group." The notion that the sheer amount of data and sophistication of analysis is so great as to limit a firm with a market capitalization of $400 billion (roughly the same as Norway's GDP) from finding a way to access it easily is worrying.

Even in Europe, using access rights to find out what firms *actually* process about you—usually highly fine-grained data about your habits, behavior, and location that you might not have imagined they even had—is bewildering and time-intensive. First, you have to prove your

identity, cope with countless attempts to defuse your request, and petition the EU regulator to take your concerns seriously. After that, you might get either an arbitrary selection of data (often in a lengthy but nevertheless incomplete PDF) or a legally suspect dead-end refusal. The penalties for violating European data protection law are now high, so if it applies to you and you truly know how to push, companies might give eventual consideration to your concerns.

But in the U.S., there is no data protection authority to back you up. The idea that the voluntary "controls" Zuckerberg invoked will truly shine light on shadowy profiling practices is almost laughable. Facebook is far from the only villain: Similar "we can't find your data, but a hacker could" excuses are commonly rolled out by even privacy-protective companies such as Apple, which stores all audio and transcripts users dictate to Siri for analysis but stubbornly refuses to provide user control.

Facebook claims that access to such detailed data is not of use to the average consumer. *Let us run our algorithmic systems over it*, company leaders say, *and we will give you a basic overview of the result*. It's true that not all consumers are interested in or have a use for gigabytes of information about themselves. But that shouldn't be an excuse to let the firm paint a rosy picture about its tracking practices and the inferences they enable on both users and nonusers. Transparency around complex data and processing practices is useful, particularly to regulators and to civil society groups, who translate that information and ignite true public debate.

If Facebook truly wanted to, it could give "joint data controller" status to Facebook Ireland with regard to U.S. and Canadian users as well as the 89 percent it currently serves. This would give all Facebook users recourse to justice, enforcement of the GDPR, and legal rights beyond that of Zuckerberg's promised "controls." Yet it's easy to imagine that politicians like Sen. Ted Cruz—who in 2016 claimed that a largely bureaucratic change involving the organization that assigns domain names was tantamount "to giv[ing] away control of the internet"—would bristle at that: Why should European courts determine the remedies available to American residents, for an American firm? Better would be to pass a similarly strong piece of legislation in the U.S. The global data protection agreement Convention 108, whose signatories extend beyond the European Union and the content of which is currently being modernized, provides a good start for this process. If the U.S. wants to steer the direction of digital policy in the global arena, it needs to step up to, not back from, the regulatory table. •