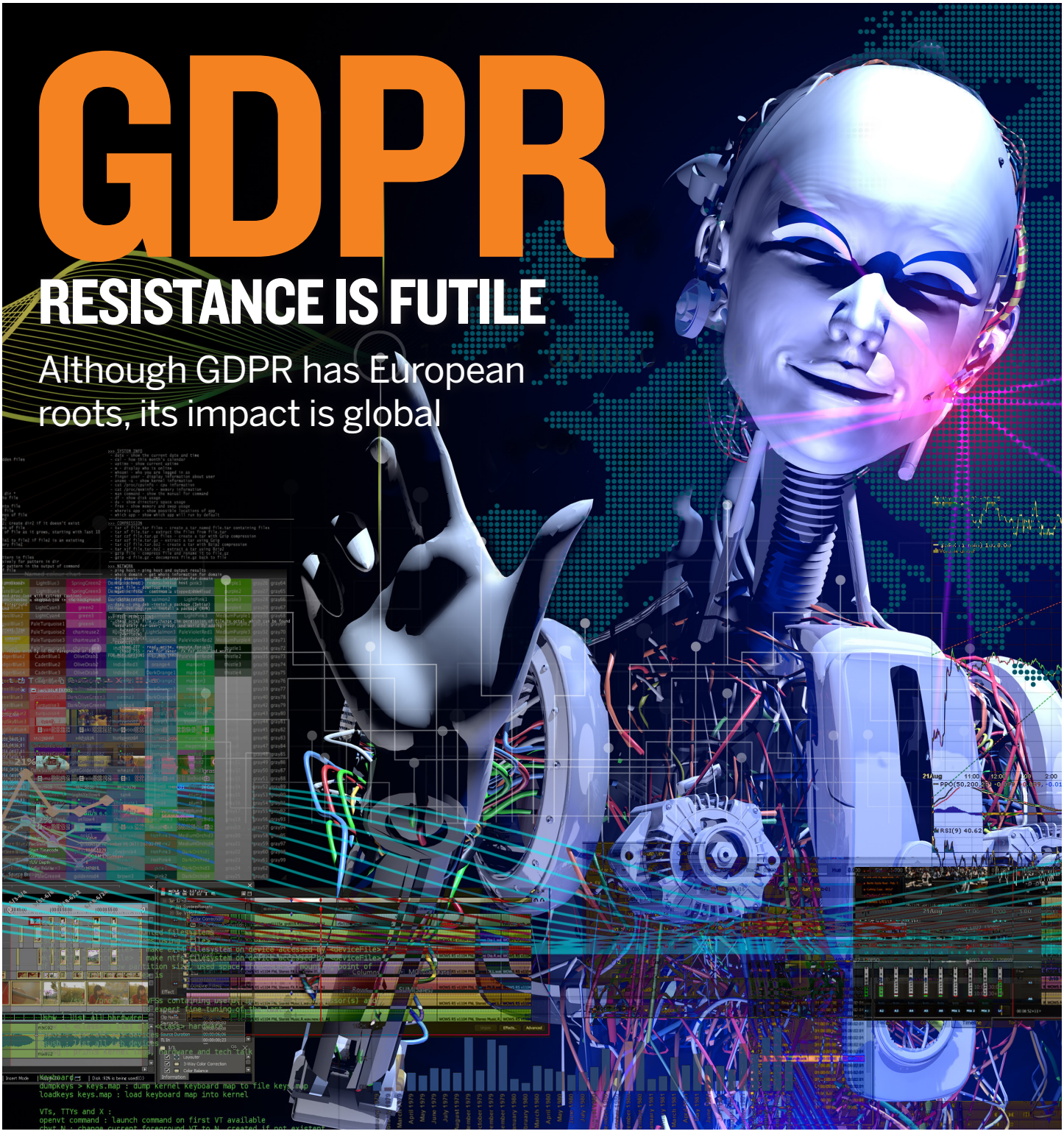
GDPR

RESISTANCE IS FUTILE

Although GDPR has European roots, its impact is global



ebook

An SC Media publication

Sponsored by

RSA®

Privacy is the next security frontier

GDPR's regulation are all about privacy, but it will have a worldwide impact on information security practices, policies and procedures. Evan Schuman reports.

When the European Union's General Data Protection Regulation (GDPR) goes into effect May 25, 2018, it will have a massive impact on privacy and security approaches for companies all over the world. But many large U.S. companies appear to be delaying their compliance, at least based on the massive number of American firms that have yet to start preparing for GDPR.

There are quite a few reasons for this lack of action, ranging from ignorance of how the regulation will apply in North America to a wait-and-see approach where companies will want to see where EU regulators and various auditors are focusing their efforts before beginning in earnest their own GDPR compliance efforts. And some companies legitimately are skeptical that the EU's GDPR fines would be enforceable on an overseas company.

Many GDPR experts, however, believe those reasons miss the point. Given that GDPR consists primarily for privacy regulations and only secondarily on security, the argument goes, why not opt for compliance? Even if a company has no obvious business interests in EU countries (no customers, no employees, no contractors, partners or operations), these rules are likely to be mimicked by regulators in Canada, Australia, Japan and other countries, as well as privacy-concerned U.S. states including California and New York. But even if that is not enough of an incentive to comply with GDPR regulations, there are others that are applicable.

If a large U.S. company has none of those customer/employee/partner interests in EU countries, GDPR could still apply, according to the regulation's wording. GDPR focuses on protecting the privacy of EU citizens as well as EU residents wherever that data might reside. That means that if any data from any citizen of the EU (who could easily be living elsewhere, including the U.S.) happens to be among your customers or employees, GDPR has jurisdiction.

This very much includes anyone simply visiting the company's Web site. Once they visit, they leave trails of IP addresses and other personally identifiable information (PII) and that is one of the components that GDPR protects. A company could therefore choose to not sell — and certainly not to ship products — to anyone in an EU country, but if one of those EU citizens simply visits the site, that company has protected data covered by GDPR.

What if the company simply chooses to block any IP addresses from EU countries? That might help, but an EU citizen could use a privacy browser such as Tor or any VPN and could mask their true IP addresses

OUR EXPERTS: GDPR

Dasha Cherepennikova, chief strategy officer, One World Identity
Eric Dieterich, privacy consultant
Alexander García-Tobar, mentor at the Center for Entrepreneurship & Technology at the University of California at Berkeley and CEO of ValiMail
William T. Kellermann, technology attorney, HansonBridgett
Richard Stiennon, director, International Data Sanitization Consortium
Donna Taylor, security consultant
Debbie Zaller, the privacy leader of security compliance assessor Schellman & Company

GDPR

>4000

Number of amendments submitted to the EU Parliament's Civil Liberities Committee about GDPR

– Global Banking and Finance Review

and appear to be coming from a non-EU country. Or that citizen could be traveling to a non-EU country and visit the company's site that way.

Using such an IP-misdirecting browser or VPN is not that uncommon in EU countries, says security consultant Donna Taylor. "They'll often use different IP addresses to get access to movies that they couldn't get access to in Germany, for example," Taylor says. "It is my observation that Americans are not sufficiently preparing (for GDPR) because they believe" they are not required to do so.

Alexander García-Tobar, CEO, ValiMail

Taylor says these large companies often enter new countries or regions and execute the minimal security and privacy requirements. "With the GDPR, you have to flip this on its head. We can't go with the least common denominator anymore," she notes. "If they procrastinated with PCI (Payment Card Industry Data Security Standard) and everything else, they will have a very steep learning curve" to achieve GDPR compliance.

Privacy consultant Eric Dieterich echoes those thoughts and says that many U.S. CISOs will be in for a shock when they try and tackle the complexities of GDPR. "The compliance standards required by GDPR are polarizing and confusing at best, with many companies in the EU struggling with the challenges around inconsistent interpretations of requirements," Dieterich notes. "Even the registration of a warranty card could bring them into scope for GDPR. GDPR establishes the fundamental privacy practices that all organizations should consider."

> "Even the registration of a warranty card could bring them into scope for GDPR."
>
> – *Eric Dieterich, Privacy consultant*

Taylor argues that many U.S. companies are still trying to be compliant with Privacy Shield, the successor to the Safe Harbour regulations that were thrown out by the EU's highest court.

"Some company executives believe that if they're compliant with the provisions of Privacy Shield, then they're likely to be covered under the GDPR as well. This misunderstanding — or willful ignorance — belies an oft-used strategy in which companies have asked for more time to be in compliance or merely gotten a slap-on-the-wrist," Taylor says. "The fines were often not painful enough to deter future misconduct. Others are in denial as to an individual EU citizen's consumer rights, especially since those rights are currently being eroded in the U.S. for its own citizens."

As to the issue of whether EU officials are going to bother chasing down non-compliant U.S. companies when they will likely have almost a full continent of local violators to deal with, Taylor says it is politically easier to punish outsiders. "If they were looking to selectively enforce it, they are more likely to selectively enforce it for someone outside the EU," she says. "They are looking for deep pockets."

A point made repeatedly among GDPR experts is that GDPR — because of its wide scope and huge geographic coverage — could become a sort of a litmus test for a company's overall privacy and security position. That could be used far beyond

28%

Percentage of world-wide IT pros who said they have little or no knowledge of GDPR

– Blancco Technology Group survey

regulators, with potential partners, potential customers and even potential investors using it as a heads-up.

"Startups looking for venture funding might want to consider how it would look if they are not claiming compliance with a regulation like GDPR," Taylor says. "It is a good way to test if the company's executives are good boys and girls, good corporate citizens. That's one of the things that VCs look at. They are trying to figure out how much risk they are willing to accept."

Alexander García-Tobar is a mentor at the Center for Entrepreneurship & Technology at the University of California at Berkeley, and CEO of ValiMail. "It is true that there is a wait-and-see attitude from U.S. CISOs and CIOs," he says.

García-Tobar noted that many American company executives do not appreciate how easily they can slip into GDPR non-compliance, even without any customers, partners or employees in EU countries.

It is not merely a matter of whether a company has any clients in the EU. "If you have clients who in turn have clients in the EU, it follows things, like a blockchain, all the way through," García-Tobar says. "This runs counter to American culture and to the way that we've done things in the past. Executives tend to not understand the interdependencies that GDPR assumes."

William T. Kellermann, technology attorney, HansonBridgett

García-Tobar joins other GDPR experts in saying that large U.S. companies might as well support the GDPR, as they will have to do so eventually. "If you are a large company, you are inevitably going to directly or indirectly deal with European data," he says. "The majority of the GDPR rules are common sense and companies should be doing them anyway."

Still, García-Tobar concedes the pragmatic attraction of U.S. companies waiting to see how other companies are treated, to allow competitors to be the GDPR guinea pigs.

"GDPR can potentially be costly to implement and interfere with current business processes and uses of data. There's also a lot of confusion around the final rules.

> "The majority of GDPR rules are common sense..."
>
> – Alexander García-Tobar, CEO, ValiMail

As a result, no one wants to rush into it if they don't have to," García-Tobar says. "It's like someone passed a law saying you have to wear new $500 sunglasses starting next March and if they're not the right kind, you may have to buy a second pair. Nobody is going to rush out and be the first to buy the sunglasses today. They're going to wait as long as they can to make the commitment and see what everyone else is doing."

García-Tobar adds that this is typically how new data rules are handled. "We saw this with HIPAA (Health Insurance Portability and Accountability Act). Nobody wanted to be the first to figure out all the difficulties with compliance. It's much better to wait until a bunch of other companies have figured the problems out first, so you can benefit from their hard-won experience," he says. "Besides, maybe some company will come along between now and then that makes compliance less of a hassle and less expensive than it is now."

William T. Kellermann, a technology attorney with the HansonBridgett law firm in San Francisco, points out two other non-EU reasons for companies to comply

40%

Businesses that said they would have to cut staff or go out of business if they suffered the maximum GDPR fine.

– Foregenix

with GDPR. First are contracts from customers and partners. Kellermann says he is already seeing contracts that are requiring GDPR compliance. And, he cautions, do not forget the EU potential mess from any future mergers or acquisitions.

If a company does not comply, they are "not just cutting themselves off from the EU, but from anyone who deals with the EU," Kellermann says.

> "Right now, they are just identifying low-hanging fruit."
>
> – William T. Kellermann, technology attorney,

The second worry is the U.S. Federal Trade Commission. Although the FTC has no jurisdiction to enforce a European requirement, it does have a policy of forcing companies to live up to their own words. In this case, that could signal trouble for a company that has a privacy policy pledging compliance with privacy rules worldwide and a lack of compliance with GDPR.

"So they put this in a privacy statement and then some engineer finds this trove of data and tries to repurpose it," Kellermann says, adding that orphan data — where a project is shut down but no one bothers to go in and delete all of the gathered data — is another GDPR danger area.

Debbie Zaller, privacy leader, Schellman & Company

Kellermann questions whether that many U.S. CISOs have "a realistic assessment of what it's going to take" to be GDPR compliant. "Right now, they are just identifying low-hanging fruit," he says.

He also questioned the wisdom of the strategy of companies waiting to see how others fare with GDPR regulators. "It's a bit like playing chicken. From a legal perspective, is that the right thing to do? Probably not," Kellermann says.

Another problem is financial, Kellermann notes. "Which budget pays for this? Legal? Finance? Privacy?" In a company that does not have an office of the Chief Privacy Officer — or the European equivalent of a Data Protection Officer — there might simply not exist enough unaccounted for budget to cover the non-trivial costs of GDPR compliance.

How big an effort is that compliance program for a Fortune 1000 company likely to be? Many experts believe that a company should assume that a GDPR program for a large American company to take at least a year and potentially two years to implement. (Compliance with GDPR will be mandatory in May 2018.) European companies can generally achieve compliance more quickly because they have already dealt with many of the GDPR's requirements because of Europe's historically more aggressive stance on data privacy.

"Many companies have significant volume of unstructured data sitting in decentralized locations such as end-points — laptops, desktops, mobile devices — with little control or insight into the scope of the data problem. Software, systems, programs or projects to address this data are time-consuming and expensive. Companies do not have the money, resources or talent to assess and address the issue to meet GDPR obligations," Kellermann says.

"Many of the tools used to provide cyber security are configured for a U.S. privacy regime that is not structured to protect individual privacy," he continues. "The features and functionality to configure

72 hours

The allowable time a company has to report a breach under GDPR regulations.

– European Union

the tools to meet GDPR anti-surveillance requirements either don't exist, require custom implementation or require wholesale changes to security analyst process, procedures and training."

Debbie Zaller, the privacy leader of security compliance assessor Schellman & Company, agrees that compliance will not be quick or easy. "To get the right processes and technology and training in place" will take at least a year, Zaller says. "This can't be done in three months or six months or even nine months. They know that they are going to have to do full data classification and data inventory and that will take years," she says.

Richard Stiennon, director, International Data Sanitization Consortium

Kellermann says there are also some emotional issues at play, with one set of companies feeling that they are fixing problems caused by an unrelated set of companies. "Companies carry some resentment that the GDPR appears primarily directed to address issues created by social media companies or the top tier of global high tech companies, yet create compliance problems for non-social media, or smaller B2B or non tech companies with EU operations and employees," he says.

> "This can't be done in three months or six months or even nine months."
>
> *– Debbie Zaller, privacy leader, Schellman & Company*

Indeed, some companies are resisting GDPR to the point that it is driving partnership and other organizational decisions, typically to sidestep data responsibilities for employees from or based in EU countries.

"Where the primary compliance problem is employee related, some companies have divested EU-based divisions or operations to avoid GDPR compliance issues. They then enter into strong or exclusive joint-venture relationships with the divested entity to continue revenue streams and optimal business operations," Kellermann says. "The cost of compliance is greater than the marginal revenue loss."

Richard Stiennon, the director of the International Data Sanitization Consortium, watches companies try a different kind of separation technique when dealing with GDPR. He is referring to data segmentation, where EU-related data is handled more stringently than non-EU data, an approach Stiennon dubs "a dangerous path.

"Many companies make the mistake of segregating requirements for EU data subjects from the data of their U.S. data subjects. But that is not how U.S. courts work," Stiennon says. "If you are taking more care of EU data than U.S. data, that will come up in lawsuits and enforcement actions."

And even if those legal problems didn't materialize, it would still be problematic as a company can never be certain that it has properly segmented all EU-related data. In other words, the technique designed to avoid GDPR issues could actually cause more GDPR issues.

Stiennon also suggests another financial reason for the apparent lack of U.S. GDPR activity in 2017. "It has to do with budget cycles. Why prepare now when the regulation goes into effect next year? As January 1 approaches, this will change dramatically," he says. "There is going to be a surge in activity that I believe will match the scramble to prepare for Y2K."

52%

Percentage of global IT professionals who think they will be fined due to GDPR violations

– Ovum

But do not interpret that comment to mean he thinks most large U.S. companies are ready to begin the GDPR compliance process. Indeed, he estimates that only half of the companies that need to embrace GDPR have done so.

"I suspect the real number is much lower as there are so many components of this 261-page regulation. Companies in France and Germany are the most prepared because they have had national regulations that already enforce many of the GDPR requirements," Stiennon says. "I have not talked to a single company that is prepared to erase records and certifiably report that erasure within 30 days as required by GDPR."

Dasha Cherepennikova, chief strategy officer, One World Identity

Another GDPR observer is Dasha Cherepennikova, the chief strategy officer at analyst firm One World Identity. Cherepennikova sees the U.S. industry, in effect, self-regulating GDPR in the sense that companies that are GDPR compliant won't want to do business with a company that isn't. "We will see lots of companies wanting to protect their own reputations and business risks" by dealing only with companies that claim GDPR compliance, she says.

Part of the issue, though, is that the current GDPR requirements have no mechanism to certify compliance. If a company is found to not be compliant, the EU can issue a fine, but if a company appears to be in compliance, nothing happens. "Nothing gives you a stamp of compliance. There is no gold star that says you are GDPR compliant," Cherepennikova says, although there have been some preliminary discussions about having third-parties doing just that.

Finally, Stiennon underscores an important point that often is forgotten when discussions turn to regulations and regulators: "regulations are not enforced by regulators, they are enforced by auditors." Auditors of all stripes will be asking for GDPR compliance as an indicator of corporate good citizenship.

Ultimately, the question for corporate officers is simple: When you are faced with an auditor asking you questions about your compliance or lack thereof when it comes to GDPR, will you be ready to respond? Many of the new rules and regulations that govern corporate responsibility and executive accountability could impact your answer. ■

For more information about ebooks from SC Media, *please contact Stephen Lawton, special projects editor, at stephen.lawton@haymarketmedia.com.*

If your company is interested in sponsoring an ebook, please contact David Steifman, VP, publisher, at 646-638-6008, or via email at david.steifman@haymarketmedia.com.

1984

Year that the UK's Data Protection Act was passed; earliest forerunner of GDPR

– United Kingdom government