CDM

CYBER DEFENSE MAGAZINE

THE PREMIER SOURCE FOR IT SECURITY INFORMATION

eMAGAZINE

INSIDE THIS EDITION

Cyber Resilience: The Real Battle…

Deception Technology for Active Defense

Five Reasons CISO's Fail

Managing Digital Authentication Credentials

Top 10 Tricks to Avoid Malware

The Internet of Things Predictions

Why is Cybercrime a Big Threat in IoT Era?

Why VPNs Are More Than Just Security Apps

and much more…

SPOTLIGHT

Six Essential Questions About "ePrivacy"

by Alex van der Wolk
Privacy + Data Security Group Global Co-Chair
Morrison & Foerster

DECEMBER 2018

MORE INSIDE!

Six Essential Questions About "ePrivacy"

by Alex van der Wolk, Privacy + Data Security Group Global Co-Chair, Morrison & Foerster

In the realm of privacy and personal data, 2018, thus far, has been all about the General Data Protection Regulation (GDPR). We have seen more talk about consent, privacy notices, access requests and data protection officers in this year than we've seen in the last decade. For many, the GDPR has meant a substantial investment and reform of their business practices. I would love to say that that's it, but the truth unfortunately is that there is a tail to the privacy reform which not everyone may be aware of. That tail is the new EU ePrivacy Regulation that governs certain forms of marketing and the use of cookies and other online technologies. Here are six things everyone should be aware of.

1. What is this ePrivacy all about? Unlike GDPR, which regulates everything that has to do with personal information, ePrivacy has a more narrow, yet more specific scope of application. ePrivacy regulates certain forms of digital marketing, such as email, but also SMS and soon possibly also marketing via messenger services such as Whatsapp. But that's not all. All the cookie pop-ups you've been seeing on websites over the years? That's also ePrivacy. And in that domain the requirements are to be expanded also (think device fingerprinting, pixel (re)targeting and any other technology facilitating online tracking and conversion). And then there's a new area ePrivacy is set to regulate, namely where digital marketing intersects with "brick and mortar", such as beacon advertizing, wifi tracking, bluetooth marketing – technologies that rely on the proximity of devices.

2. But doesn't GDPR already cover all of this? Well, yes and no. The title ePrivacy may be a bit off-setting here. Unlike GDPR, which applies to anything that has to do with personal information (regardless of the technology used), ePrivacy rather regards just the technology. In fact, for ePrivacy, it doesn't really matter whether personal information is at stake or not. The mere use of a covered technology may already qualify you for ePrivacy applicability. This also highlights the real tricky part about all of this: it is very well possible that ePrivacy and GDPR apply both at the same time. If you engage certain technology that is covered by ePrivacy AND that use also involves personal information, you may have to comply with both ePrivacy and GDPR.

3. So is ePrivacy just about getting more consents? Consent certainly is a firm cornerstone of the ePrivacy Regulation. Most of us are familiar with the current consent (opt-in) requirements for email marketing and the use of cookies on websites. This will remain in place. However, in order for consent to be valid going forward, it is unlikely companies will be able to (continue to) rely on implied or inferred consents. Like GDPR, ePrivacy will require consents to consist of a "clear affirmative act" from the individual. So, for example, in the context of cookies, relying on the continued use of a website to constitute acceptance of cookies is unlikely to be sufficient anymore.

Speaking of cookies, the ePrivacy Regulation may also contain a specific prohibition on cookie walls: denying access to a website, service, or functionality when the user does not provide consent will not result in valid cookie consent. And once any consent is obtained, the ePrivacy Regulation will likely require companies to remind the individuals of the option to withdraw consent at periodic intervals of either six or twelve months.

But it is not just about more consents. For example, the legislative proposals also suggest imposing an obligation on companies to offer online privacy settings (such as privacy dashboards) through which users can set and manage their online privacy preferences. Building such privacy dashboards would not only be a costly affair for any company, but could bring along a host of other issues. This may be one of the reasons that it is still in flux whether this obligation will make its way into the final text of the ePrivacy Regulation.

4. Does ePrivacy say anything about marketing phone calls? Yes, the ePrivacy Regulation will also cover telephone-based marketing. The legislative proposals suggest that voice-to-voice calls should only be allowed if the recipient has not opted out. This doesn't necessarily suggest an opt-in for marketing calls, but it does make sure that individuals have an opportunity to un-list from being approached by phone for commercial purposes. Many EU countries currently already provide for a similar requirement. In addition, companies conducting voice-to-voice calls may also have to adopt new transparency tactics, such as displaying their calling numbers and using a specific code or prefix identifying the call as a marketing call.

5. So what are the risks? Like GDPR, the ePrivacy Regulation will also bring about substantially higher fines. The legislative proposals mention fines that could run up to 2% of a company's total worldwide annual turnover or €10 million (whichever is higher).

However, unlike GDPR, the ePrivacy rules don't mind where a company is established, but rather where the individuals (the recipients of emails, visitors to your website, etc.) are located. So even if your company has no physical presence in the EU, the ePrivacy Regulation may still apply, particularly if you market to individuals in the EU, or use cookies and/or similar technologies on their devices.

6. Where do we go from here? The ePrivacy Regulation is still a work in progress. It is uncertain when it will be finalized, but the latest prognoses are for end of 2018/early 2019. What is certain is that once ePrivacy is finalized, companies will have a one-year transition period to implement the new rules. Companies are advised to start their ePrivacy compliance programs on time.

About the Author

Alex van der Wolk is the global co-chair of law firm Morrison & Foerster's Privacy + Data Security Group. Based in Brussels, he focuses on data protection information/communications technology law and advises global companies on data protection strategy and compliance governing all aspects of information management. Alex can be reached online at avanderwolk@mofo.com and on Morrison &

Foerster's website: https://www.mofo.com/people/alex-van-der-wolk.html.