ELECTRONIC COMMUNICATIONS

ePrivacy

WHITE PAPER

PREPARED BY

CRANIUM PRIVACY & SECURITY

CRANIUM

www.cranium.eu

MANAGEMENT SUMMARY

Faced with multiple drafts of the ePrivacy Regulation from the European Commission, Parliament, Council and the Romanian Presidency and stalled by numerous issues, including: significant lobbying efforts, upcoming European Parliamentary elections and the invariable challenge of synthesizing law, business and technology, it is often difficult to understand where the European rules on electronic communication currently stand, what are the proposed changes, who they will affect and how. This is only confused further by the onset of additional European legislation, such as the European Electronic Communications Code, which also imposes rules on certain data processing activities.

What follows is a comprehensive assessment of the ePrivacy Regulation, in an attempt to shed light on the implications of all the different versions proposed by the various European entities and draw out practical conclusions for the reader.

To achieve this overview, the paper is structured so as to follow the key requirements of ePrivacy as stated by the European Commission, namely:

- Territorial Scope
- Material Scope
- Confidentiality of Communications – *including Cookies, protection in transit/after receipt and Internet of Things*
- Security of networks and services
- Data breach notifications
- Traffic and location data – *including telecommunications and metadata*
- Spam – *including (electronic) marketing*
- Public Directories
- Calling-line identification
- Penalties

In the case of each subsection, there will be an assessment of the relevant rules in each of the 2002 ePrivacy Directive (currently in force) and the proposed ePrivacy Regulation, outlining the tensions between the different draft proposals from the European Union. This is intended to help clarify how the rules are changing and what their consequences are for in scope organizations.

Where relevant, this paper will also assess those parts of the new European Electronic Communications Code, already in force, that have a bearing on the rules on ePrivacy.

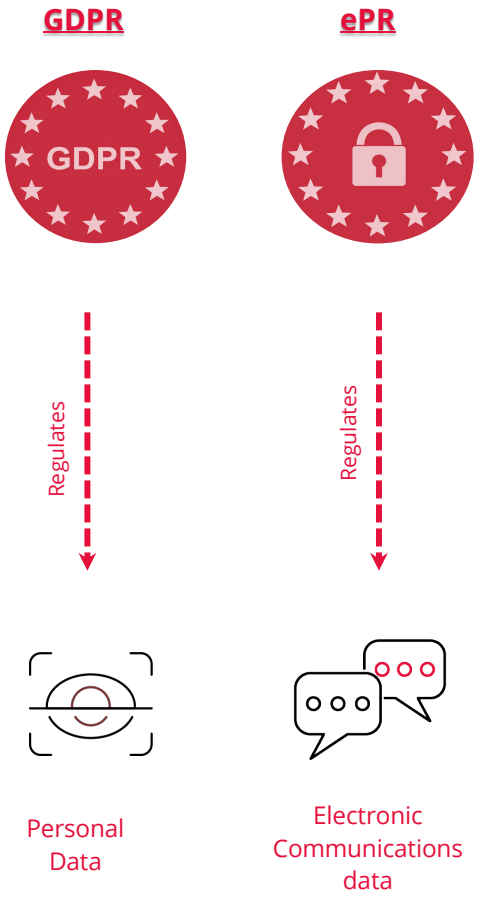
Ultimately, the overriding conclusion is that, the lack of clarity polluting the rules on electronic communications provides all the more cause for organizations to start reviewing their use of electronic communications data, services and networks sooner rather than later. The one thing that is certain about the ePrivacy regulation, is that it promises to be a significant compliance challenge for most companies, and since important business operations (such as marketing) are affected by this legislation, it is imperative to commence planning compliance projects and actions immediately to ensure minimal impact and maintain optimal business performance.

DIGITALIZATION REQUIRES NEW LEGISLATION

The General Data Protection Regulation (hereinafter GDPR), enforced in May 2018, represents only the **first of several actions** by the European Union to update its legislative framework for data protection to ensure the law remains relevant and effective in the wake of digitalization.

In this respect, there are two further upcoming pieces of European legislation of which organizations need to be aware: The **ePrivacy Regulation** (hereinafter **ePR**) and the **European Electronic Communications Code** (hereinafter **EECC**) both of which are discussed in greater detail below.

Why ePrivacy?



BECAUSE THE GDPR IS NOT ENOUGH

Whilst there is certainly some overlap between the two sets of legislation, **ePrivacy is not the same as the GDPR**. The GDPR concerns personal data in general. The ePR, more specifically, concerns **electronic communications data**. This means that the ePR is *lex specialis* to the GDPR: i.e. where the ePR stipulates more specific or stringent requirements for a particular topic than does the GDPR (e.g. regarding cookies which are governed by both the GDPR and the ePR), it is the ePR that takes precedence.

A new ePrivacy law is necessary to ensure proper protection of the end-user in the digital age – which the GDPR alone is insufficient to accomplish. This is because the GDPR does not regulate communications *per se* (unless they contain personal data), which comprise a significant privacy concern. Whereas traditional telecoms providers (such as Vodafone) have long been restricted from snooping or collecting confidential communication

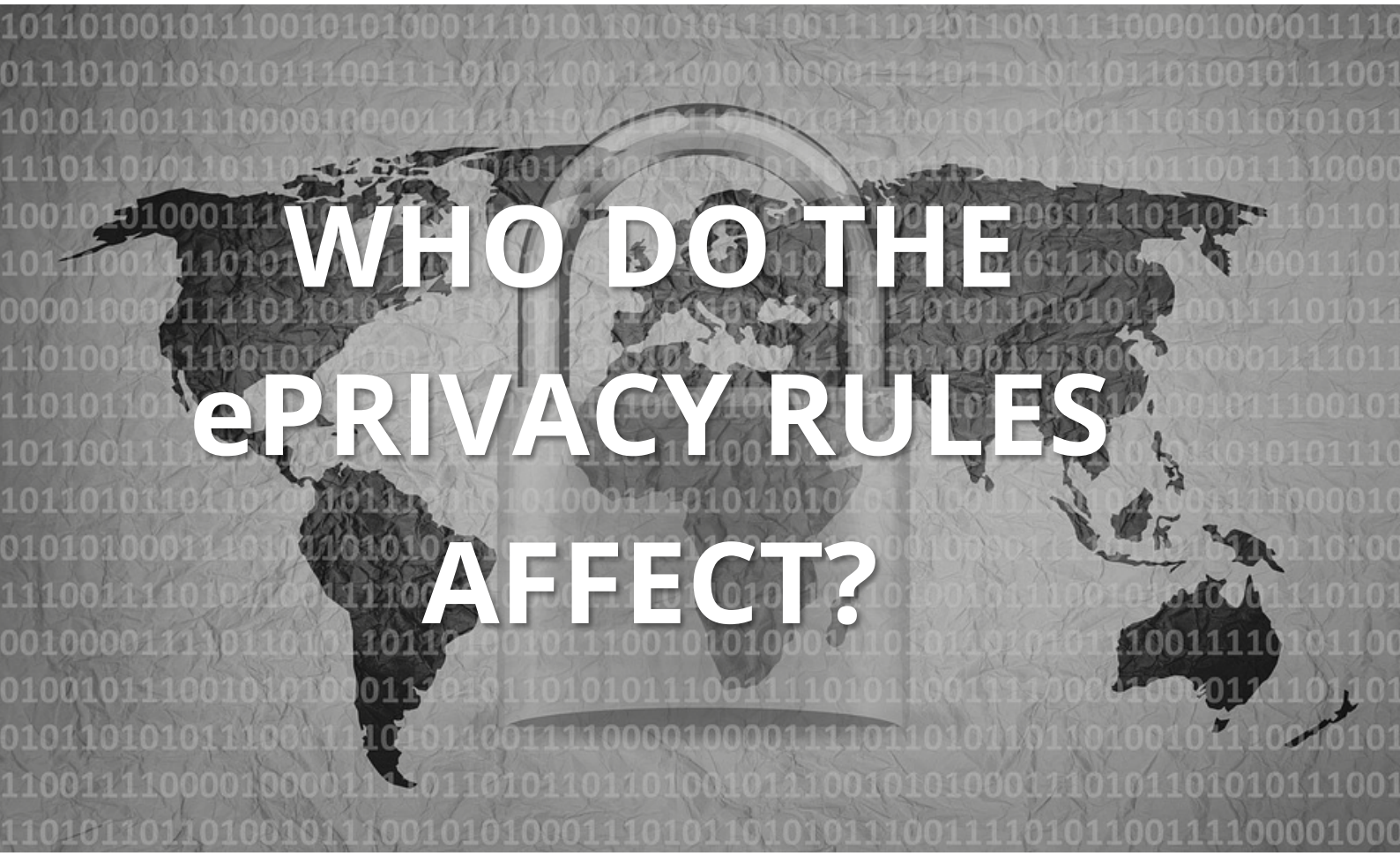
information, no such boundaries have been placed on **Over the Top** providers (hereinafter **OTTs**) such as Whatsapp and Messenger, thereby seriously undermining the privacy of individuals in the 21st century. In recognition of this legislative shortfall, the Commission have already adopted a new EECC to ensure that modern providers of communications services are already brought into scope of EU data protection law, as is discussed in greater detail below.

The ePR is intended to update and replace the 2002 ePrivacy Directive, but it has yet to complete the legislative process, with multiple parties challenging various elements of the proposed regulation. This means it is unlikely that the ePR will enter into force until 2020.[1] Nevertheless, with extensive changes being made to the rules on processing electronic communications data, **in scope organizations need to act sooner rather than later**.

The proposed changes to the rules on ePrivacy are outlined below and can be surmised as follows:

- Territorial Scope
- Material Scope
- Confidentiality of Communications
- Security of networks and services
- Data breach notifications
- Traffic and location data
- Spam
- Public Directories
- Calling-line identification
- Penalties

[1]This is CRANIUM's prediction, based on a comparative review of the ePrivacy drafts proposed by the European Commission, European Parliament, the European Council and the Romanian Presidency, including assessment of the extent of their alignment, and including consideration of the upcoming European Parliament elections.



WHO DO THE ePRIVACY RULES AFFECT?

TERRITORIAL SCOPE

ePrivacy Directive 2002

Territorial scope in the original 2002 ePrivacy directive is defined only in reference to the 1995 Data Protection Directive[2]: *"The provisions of this Directive particularise and complement Directive 95/46/EC for the purposes mentioned in paragraph 1."* In other words, the territorial scope of the ePrivacy Directive is aligned entirely with the 1995 Data Protection Directive.

However, given that the 1995 Data Protection Directive was repealed and replaced by the GDPR[3], the territorial scope of the current ePrivacy directive will need to refer to the GDPR to remain relevant – at least until the European Union reaches a consensus on the new ePrivacy Regulation.

[2] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), Official Journal L 201, 31/07/2002 P. 0037 – 0047.

[3] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32016R0679.

ePrivacy Regulation

In contrast to its predecessor; the proposed ePR[4] establishes an explicit territorial scope and is intended to apply to the following:
"(a) The provision of electronic communications services to end-users[5] in the Union, irrespective of whether a payment of the end-user is required;
(b) the use of such services;
(c) the protection of information related to the terminal equipment of end-users located in the Union."

In other words, territorial scope of the ePR is determined in relation to **the location of the end-user in the Union**. Whether the company itself that offers the services to the end-user is located in the Union is irrelevant. This marks a departure from the GDPR, which establishes territorial scope for organizations outside the EEA on the basis of the location and purposes of the personal data processing rather than according to where the end-user/data subject resides.

For example, under the ePR, an individual residing in France would benefit from its protection such that any American third-parties would be prevented from collecting or storing information from/on his terminal equipment, simply by virtue of the fact that his equipment is in Europe. By contrast, under the GDPR, an individual residing in France using his terminal equipment to surf the web, who lands on an American website (but which is <u>not</u> targeted at Europe *per GDPR*) would receive no such protection for any personal data that may be collected by the American website provider. This provides a clear example of how GDPR compliance will be insufficient to ensure ePR compliance and why **organizations will need to consider both laws in tandem**.

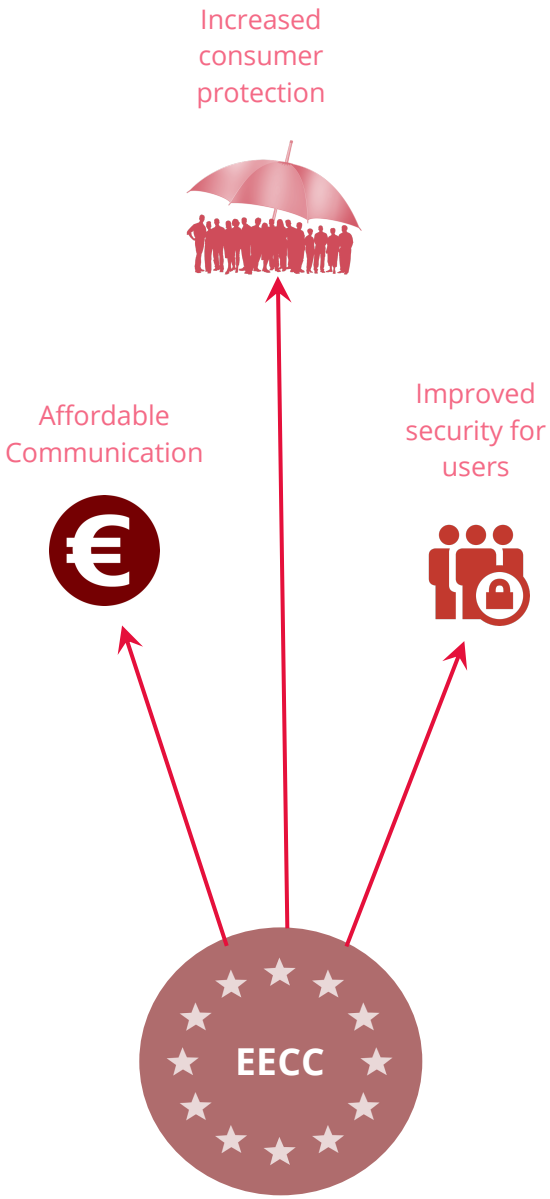
[4] Proposal for a regulation of the European parliament and of the council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), 10.01.2017.
[5] Definition of end-user: a user not providing public communications networks or
publicly available electronic communications services. (Proposal for a directive of the European parliament and of the council establishing the European Electronic Communications Code (Recast) COM/2016/0590 final - 2016/0288 (COD))

European Electronic Communications Code[6]

In addition to the ePR, the Commission adopted a new EECC Directive which establishes new rules to increase consumer protection and security for users, ensure affordable access to communication for individuals and prepare the ground for the unrolling of 5G across the Union.

Territorial scope is not explicitly stated in the EECC. As a directive, it inevitably applies to all Member States and communication providers in the Union. However, it is uncertain as to whether the EECC will establish a scope to match that of the GDPR or the ePR, whereby organizations established outside the EEA targeting electronic communication networks and services into the Union are caught by the EECC requirements, or whether it applies purely to providers established inside the Union.

Given that the EECC extends European telecommunications rules to OTTs, it would be incongruent were the territorial reach of the EECC to be restricted to those providers with a European establishment. The largest OTTs (think Whatsapp, Snapchat), having their establishment outside of Europe, would avoid compliance with the EECC requirements completely. It is more likely that, in practice, the EECC will be territorially applied in a manner aligned to that of the ePR and/or the GDPR.



[6] http://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_BRI(2016)593562 (consulted 8 February 2019)

MATERIAL SCOPE

ePrivacy Directive 2002

The 2002 ePrivacy Directive applies only to the processing of personal data in connection with the provision of publicly available electronic communications services in **public communications networks** in the Community, including public communications networks supporting data collection and identification devices.

However, intended to regulate the processing of electronic communications data, it is clear that the limited scope of the 2002 ePrivacy Directive is ill equipped to address the changes created by technological advances whereby the processing of electronic communications data is no longer restricted to publicly available electronic communication networks used by traditional providers of communications services.

FACT: The scope of existing ePrivacy rules have **already** been expanded via the EECC, such that **OTTs must comply** with *current* ePrivacy requirements *irrespective* of what happens with the new ePR.

ePrivacy Regulation

For this reason, the January 2017 draft of the new ePR proposes a **much broader scope** of application:

This Regulation applies to the processing of electronic communications data carried out in connection with the provision and the use of electronic communications services and to information related to the terminal equipment of end-users.

Whereas the Directive explicitly refers to public communication networks, the Regulation (via the EECC) extends its scope to include electronic communications services.[7] This is much broader, as electronic communications services encompass (i) **internet access services**, (ii) *INTERPERSONAL COMMUNICATIONS* and (iii) transmissions that use an electronic network. This expansion in scope more accurately reflects how electronic communication data[8] is processed in the 21st century, with OTTs such as Skype, Whatsapp and Messenger all falling within the category of *interpersonal communications,* and machine-to-machine communications (hereinafter M2M) being caught by *transmissions that use an electronic network*. Consequently, providers of communication services over the internet and the IoT sector will be the most affected by the legislation, with traditional telecommunications companies gaining a head start on account of their historic compliance with the 2002 ePrivacy Directive.

[7] (Article 4, European Electronic Communications Code)

[8] Electronic communications data means both Electronic communications content and -metadata. 'Electronic communications content' means the content exchanged by means of electronic communications services, such as text, voice, videos, images, and sound;
'Electronic communications metadata' means data processed in an electronic communications network for the purposes of transmitting, distributing or exchanging electronic communications content; including data used to trace and identify the source and destination of a communication, data on the location of the device generated in the context of providing electronic communications services, and the date, time, duration and the type of communication (Proposal for a regulation of the European parliament and of the council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), 10.01.2017)

European Electronic Communications Code (EECC)

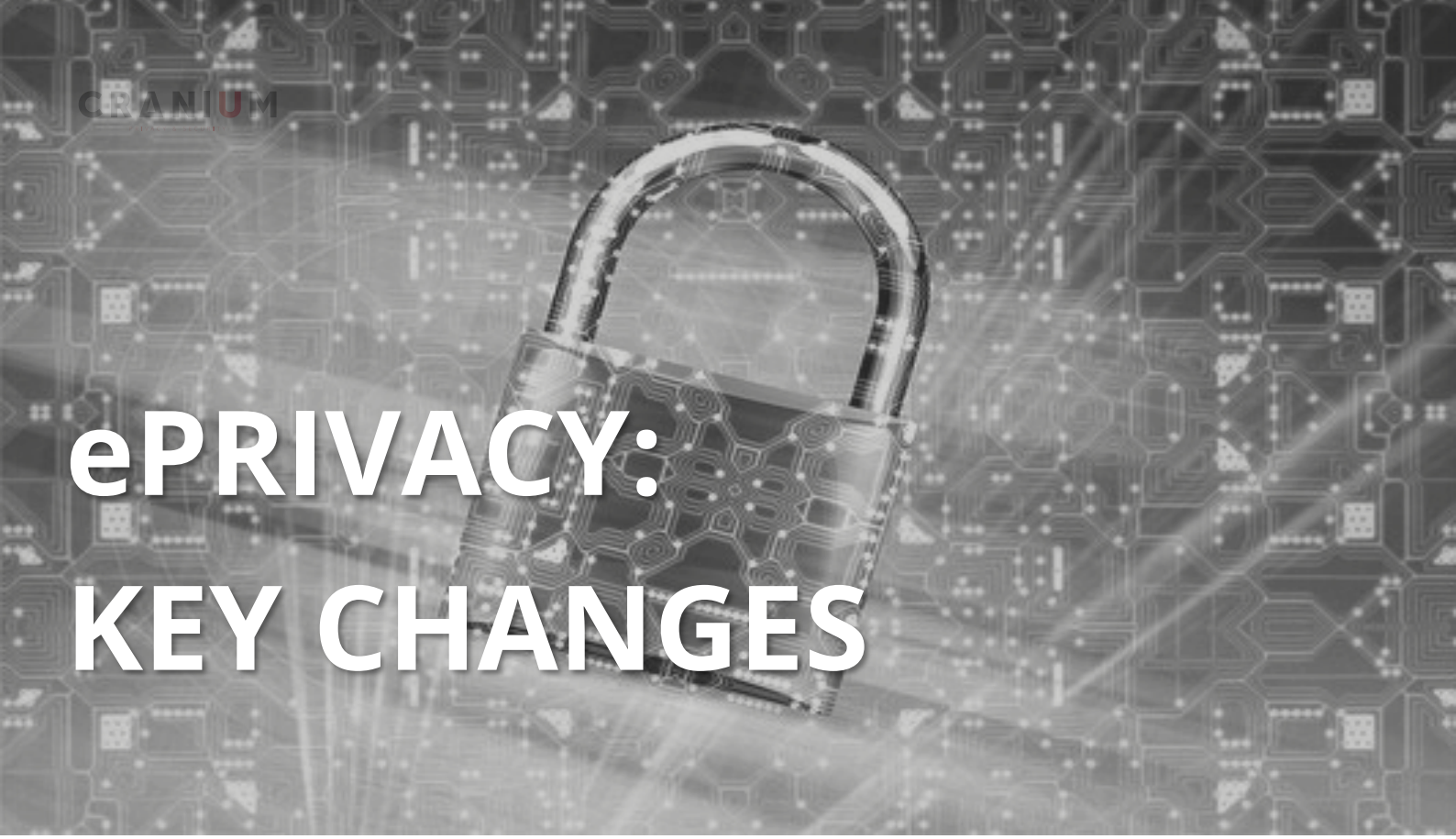
To reinforce this position in the ePR, the EECC elucidates that where communication services are provided **in exchange for remuneration**, they qualify as electronic communications services and therefore fall in scope of both the EECC and ePR. Under the EECC, 'remuneration' can include personal data and/or acceptance of advertising conditions.[9] Whilst this leaves no doubt that the broadened scope of the new European privacy framework is intended to curb the surreptitious practices of modern tech and big data companies, it nevertheless creates a direct conflict with the principle of 'freely given' consent in European data protection law and reveals further inconsistency in the legal concepts underpinning modern data protection legislation.[10]

OTT providers should note that the EECC will be enforced from the **21 December 2020**. This is important because the EECC ensures that the 2002 ePrivacy directive currently in force **already applies to OTT providers**[11] and not simply to traditional telecommunications providers. Consequently, OTTs should *not* rely on the delay in ePR to start complying with some of the requirements set out in the directive as the EECC ensures that OTTs are caught in scope of ePrivacy even before the new ePR becomes law. Companies who implement compliance solutions for both ePR and EECC in parallel will have the advantage of killing two birds with one stone, thereby reducing compliance costs and dedicated resources. Those companies who only seek to conform as each piece of legislation becomes official will have to overhaul their compliance for each new law, unnecessarily exaggerating the overall compliance costs.

[9] https://legalnews.be/privacy-it-ip-recht/informaticarecht/the-european-electronic-communications-code-is-now-in-force-10-takeaways-stibbe/ (Consulted 15 February 2019)

[10] Furthermore, the concept of providing personal data as a form of remuneration requires in law for there to be a property right tied to the personal data, which is not the case. This only adds to the legal uncertainty of the provision.

[11] OTT services include internet access services, interpersonal communications services and services consisting wholly or mainly in the conveyance of signals.



ePRIVACY: KEY CHANGES

WHAT YOU SHOULD KNOW

Whilst colloquially referred to as the cookie law, the European Commission emphasizes that the ePrivacy directive regulates far more than simply cookies:

1. **Confidentiality of communications**: EU Member States must ensure the confidentiality of communications over public networks, in particular by prohibiting the listening into, tapping and storage of communications without the consent of the users concerned.
2. **Security of networks and services:** a provider of a public electronic communications service has to take appropriate measures to safeguard the security of its service.
3. **Data breach notifications**: if a provider suffers a breach of security that leads to personal data being lost or stolen, it has to inform the national authority and, in certain cases, the subscriber or individual.
4. **Traffic and location data:** this data must be erased or made anonymous when no longer required for communication or billing purposes, except if the subscriber has given consent for another use.
5. **Spam**: subscribers must give their prior consent before unsolicited commercial communications ("spam") are addressed to them. This also covers SMS text messages and other electronic messages received on any fixed or mobile terminal.
6. **Public directories:** subscribers' prior consent is required in order for their telephone numbers, e-mail addresses and postal addresses to appear in public directories.

7. **Calling-line identification**: subscribers must be given the option not to have their telephone number disclosed when they make a call.[12]

The fact that the 2002 directive stipulates multiple requirements that extend far beyond cookie use means that telecommunications and OTT providers will need to prepare their ePrivacy compliance accordingly: **implementing a cookie notice alone will be insufficient**, and, akin to the GDPR, a holistic compliance approach will be necessary.

[12] https://ec.europa.eu/digital-single-market/news/ePrivacy-directive (consulted on 12/16/18).

COMMUNICATION IS CONFIDENTIAL

CONFIDENTIALITY OF COMMUNICATIONS

Cookies

Nevertheless, despite its broad parameters, some of the most controversial and complex changes to the ePrivacy legislation evidently center on the use of cookies and consent.

ePrivacy Directive 2002

Under current ePrivacy laws, informed, specific and freely given consent is required for storing or accessing information on a user's terminal equipment.[13] However, with the advent of the GDPR in 2018, this consent must now also be **unambiguous**. This is because the current ePrivacy directive defines consent in relation to the EU's data protection legislative framework (i.e. the GDPR). Practically speaking, this means organizations must inform users of any cookies and enable them to **actively** accept or reject them **before** they are installed. It is for this reason that individuals have been inundated with cookie banners, leading to what has been recently coined 'consent fatigue'.[14]

[13] http://ec.europa.eu/ipg/basics/legal/cookies/index_en.htm (consulted 12 February 2019)
[14] https://www.bbc.com/news/business-38583001 (consulted 6 February 2019)

Moreover, given its legislative form as a directive, the 2002 ePrivacy law was implemented to varying degrees by each Member State, creating inconsistency in cookies requirements across the Union. For example, whereas the UK'S ICO and the French CNIL have traditionally permitted companies to treat 'continued browsing by the user' as a form of cookie consent, the Dutch AP have conversely stipulated much stricter requirements, according to which cookies cannot be dropped on a browser until the user has actively accepted the cookies mentioned in the banner.[15] With the EDPB clearly stating that the stricter consent requirements of the GDPR (which apply under the ePR) are simply compulsory and **not an additional obligation**, it is clear that continued browsing of the user will not qualify as valid consent, even before a final ePR draft is agreed.

ePrivacy Regulation

Consequently, the proposed ePR has two major objectives regarding cookies:[16]

Simplify the cookies rules

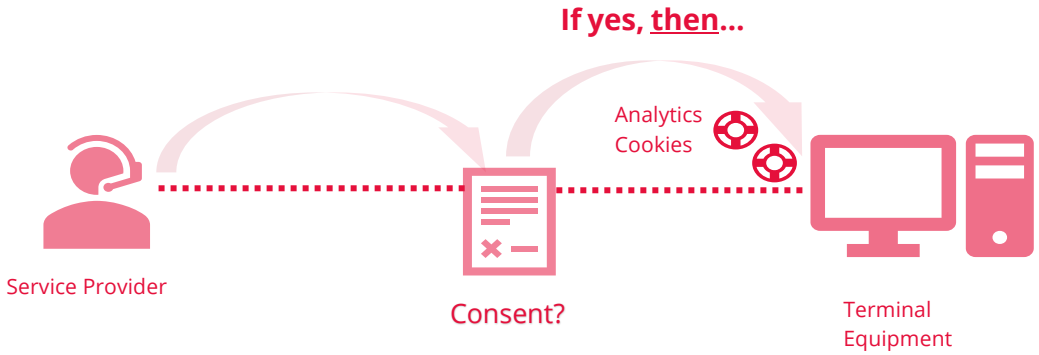
Unclear drafting of certain provisions, combined with legal ambiguity in the ePrivacy Directive, have made it difficult for organizations to be certain[1] of their obligations when operating online identifiers in more than one jurisdiction. **Transposing ePrivacy law into regulation form should lend greater consistency to the regime**, as the ePrivacy requirements will become directly applicable in each Member State. This should (theoretically) reduce the margin of variation and render obligations much clearer for organizations wishing to drop and access cookies on a user's terminal equipment. However, just as the GDPR promised standardization across the Union whilst simultaneously enabling Member States to diverge on particular provisions (such as what age constitutes 'a minor') in practice, it is unlikely that we will have a **completely** level playing field in the *post ePR era*.

Streamline cookie consent

In a bid to reduce the consent fatigue perpetuated by the 2009 amendment of the ePrivacy directive, the proposed ePR of 2017 sanctions **browser settings as an appropriate method** for obtaining consent of the end-user to interfering with their terminal equipment. However, given that the recitals and articles 8 and 10 of the proposal stipulate that this consent must be given for transparent and specific purposes, it is not yet clear how this legislative change will combat consent fatigue: users will still need to be made aware of any interference and required to actively accept or reject it.[1]

[15] https://www.iabeurope.eu/eucookielaws/ (consulted 13 February 2019)
[16] Memorandum in Proposal for a regulation of the European parliament and of the council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), 10.01.2017

Practically speaking, this means that organizations using **analytics cookies** to create targeted advertising will need to obtain the ***prior*** *consent* of the end-user **before** the *cookies can be dropped* in their browser.[1] Technically speaking, this is much easier said than done, as cookie technology typically set identifiers immediately upon a user's first visit to a website. This means organizations using certain online identifiers will need to ensure they implement controls to delay the cookies being set until after they have obtained valid consent from the end-user – there are technical solutions already available to achieve this (e.g. TrustArc, OneTrust, Apple Webkit Safari technology).



Organizations relying on cookies technology will also need to consider the **effectiveness** of the compliance measures they implement. For example, common practice around cookie consent currently involves presenting website visitors with a cookies banner immediately upon arrival, asking them to select and consent to the use of cookies. However, in many cases, website visitors can continue browsing the website without selecting their cookies options or without actively consenting, thereby rendering the cookies banner superficial and redundant. This is unlikely to remain valid practice in face of the GDPR's stricter consent requirements, which mandate 'affirmative' action for valid consent, a position confirmed by the Article 29 Working Party[17]. Interestingly, both the EDPB and EPDS have condemned the use of tracking walls – commonly applied in the Netherlands to *enable* users to select their cookies preferences before any identifiers are dropped on their browser – as an *unacceptable* control for complying with the stricter consent requirements, to the extent that it undermines the concept of consent being freely given. What will be deemed an appropriate control for collecting consent will therefore depend entirely on how it is treated in practice by the supervisory authorities, who, to date, have diverged on what constitutes acceptable cookies consent practices, as mentioned above.

[17] Article 29 Data Protection Working Party's Guidelines on Consent under Regulation 2016/679, adopted on 28 November 2017, section 3.4.1, pp.17

A second issue is a lack of clarity regarding ***who is responsible for collecting*** cookie consent, an issue exacerbated by the multiple ePR drafts that have been proposed. Whereas the 2017 proposal is inexplicit as to who the responsibility falls, the July 2018 amendment clearly states that it is the responsibility of the entity that makes use of processing and storage capabilities of terminal equipment or collects information from end-users' terminal equipment, such as an information society service provider or ad network provider[18]. The ePR review by the Romanian Presidency would also seem to indicate that the providers of electronic communications services should bear the responsibility of obtaining consent for the use of online identifiers. However, until a final draft is agreed, it remains unclear as to who will have ultimate responsibility for collecting consent.

A third issue with the cookies provisions of the new ePR concerns the concept of 'interference with terminal equipment' – a concept elaborated by Recital 20 which provides the following examples:

- **Revealing details of an individual's emotional, political, social complexities;**
- **Web bugs**
- **The location of individuals by accessing the device's GPS capabilities;**
- **Tracking cookies**

However, as recital 22 underlines, there is no need for consent when the processing and storage capabilities of terminal equipment or access to information stored in terminal equipment involve no, or negligible intrusion of privacy. But **what qualifies as non-privacy intrusive?** Whilst the proposal provides several examples (e.g. cookies can be a legitimate and useful tool for measuring web traffic to a website) it is not always clear as to whether an action will be deemed privacy intrusive by the regulators.

[18] Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) - Examination of the Presidency text, 10.07.2018.

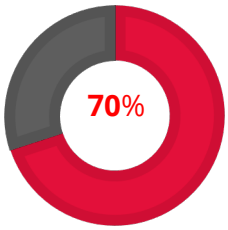
One such example involves the distinction between first and third-party analytics cookies, whereby analytics cookies can qualify as 'non-privacy intrusive', provided that they are genuinely analytics cookies rather than cookies being used to create profiles and target individuals. The Article 29 Working Party (herein after WP29) has clarified that first party analytics cookies tend not to be privacy intrusive, **provided that:**

By contrast, third party analytics cookies are, on the whole, regarded as privacy intrusive[19]. Whilst it is proper that third-party analytics cookies should not be exempted from consent requirements (as it is these types of cookies and tracking that have enabled an economy of surveillance to evolve), simply distinguishing between cookies on a first/third-party basis may be insufficient to distinguish the different privacy risks associated with each. The fact that the WP29 itself qualifies the principle of first-party analytics cookies as non-privacy intrusive with three additional criteria underlines the difficulty in distinguishing between cookies on a first/third party basis, particularly in light of current commercial cookies practices (see graphic below). The qualification of a cookie as 'first-party' is therefore insufficient in itself to determine the privacy risk that it poses – a less rudimentary distinction is required.

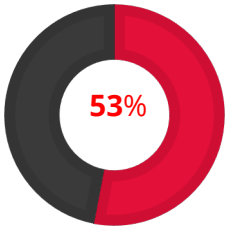
[19] Opinion 04/2012 on Cookie Consent Exemption of the Article 29 Data Protection Working Party, 7 June 2012, pp.10

It is imperative that the European Union reaches a consensus on these provisions, as it promises significant challenges for most organizations. In 2015, it was revealed by the WP29 in an assessment of **16555 cookies** across 478 websites in 8 Member States that **70% of the cookies were third party cookies**. Of the websites using these third-party cookies, ***54% did not obtain consent*** from the user.[20] Organizations should start preparing now by reviewing their cookie use and practices and identifying where they are using online identifiers to target individuals or develop profiles, whilst awaiting further clarification.

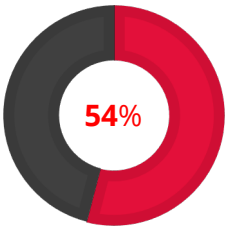
THIRD PARTY COOKIE USE IS PERVASIVE



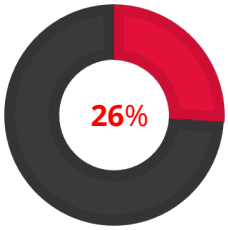
MORE THAN HALF OF THIRD PARTY COOKIES ARE SET BY JUST 25 THIRD-PARTY DOMAINS



OVER HALF OF ORGANIZATIONS DO NOT REQUEST USER CONSENT



OVER A QUARTER OF ORGANIZATIONS FAIL TO NOTIFY THE USER



[20] Cookie Sweep Combined Analysis – Report of the Article 29 Data Protection Working Party, 3 February 2015
Whilst the date of the Cookies Sweep Combined Analysis may be considered outdated from the date of writing, it remains one of the most comprehensive (published) sweeps to date and CRANIUM advises that the reported statistics are only likely to have further increased with the rapid evolution of the ad-tech sector in the years since the Cookies Sweep was performed.

In recognition of this complexity, the 2017 ePR proposal recommended that end-users should be offered the following privacy setting options:

1) **High privacy settings: e.g. do not accept cookies**
2) **Intermediate privacy settings: e.g. reject third party cookies**
3) **Low privacy settings: e.g. accept all cookies**

However, these options have been removed from the Proposal of July 2018,[21] as has article 10 and the recitals stipulating how information and options for privacy settings are to be provided. Additionally, recitals 22 – 24 of the 2017 Proposal have been replaced in the July 2018 Proposal with one recital 21a that provides an overview of the scenarios when consent is not required. Although this should help clarify which actions qualify as privacy intrusive, how this consent should be collected remains entirely unclear.

Consequently, with the rules on cookies remaining uncertain, organizations seeking to *take a proactive approach* to ePrivacy should start by **performing a litmus test** in relation to their cookie use. If an individual would be surprised to discover the use of cookies to determine certain information about them, then greater efforts need to be made around **transparency**, **PURPOSE** and ***lawfulness*** of processing. Thereafter, attempts to render cookie consent settings as *user-friendly as possible*, in the absence of concrete authority, will be the most sensible compliance position for the time being.

[21] Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) - Examination of the Presidency text, 10.07.2018.

JUST HOW UNIFORM WILL ENFORCEMENT BE?

The significance of unclear legislation becomes clear in practice when regulatory **authorities are unable to converge** on a ruling, as borne out by the two conflicting supervisory authority decisions of the ICO and the Austrian Data Protection Authority (hereinafter DPA) *regarding cookie consent* settings by online newspapers in November 2018. Whilst the decisions of the Austrian DPA and the ICO were made in relation to the GDPR, the example is still pertinent as the ePR inherits several principles and requirements from the GDPR (e.g. consent must be freely given, valid, specific, unambiguous and informed) and as both the ePR and GDPR are regulatory instruments afflicted with similar issues of legal uncertainty and uneven application.

Austrian DPA decision[22]

The Austrian DPA rejected a complaint received from an individual claiming that the cookie consent options provided by an Austrian newspaper's
website did not meet the requirements for valid consent. The cookie consent options provided by the Austrian newspaper were as follows:

a) **Accept the use of analytics and advertising cookies to receive full complimentary access to the website;**
b) **Refuse cookies and obtain limited content on the website; or**
c) **Pay a small monthly subscription (6e) to obtain full website access without any cookies or tracking technologies being installed.**

The DPA dismissed the complaint in favor of the newspaper, on the grounds that it deemed the consent solution offered by the newspaper ***compliant*** with the requirements for specific, informed and freely-given consent: individuals would not suffer as a result of the consent choices. As the DPA reasoned, individuals could either subscribe to the site for a minimal fee or select another online newspaper altogether.

[22] https://www.huntonprivacyblog.com/2019/01/07/austrian-dpa-issues-decision-on-validity-of-cookie-consent-solution/ (consulted 7 February 2019)

ICO decision[23]

Conversely, the UK ICO made an opposite ruling in relation to *similar* consent solutions offered by the Washington Post, which were as follows:

a) **Accept the use of cookies for tracking and personalization purposes to have complimentary access to a limited number of articles;**
b) **Accept the use of cookies and tracking to have a basic subscription (paid) giving access to an unlimited number of articles; or**
c) **Pay a premium subscription to gain access to an unlimited number of articles with no on-site advertising or third-party tracking cookies.**

The ICO deemed this an invalid cookie consent solution on the basis that individuals must be offered a free alternative to accepting cookies and should be able to opt-out of cookies *at all subscription levels*. This stands in direct contrast to the decision of the Austrian DPA above and illustrates the lack of clarity currently plaguing the issue of cookie consent.

Whilst the inability of both the legislators and the regulators to reach a consensus as to the proper application of consent renders effective compliance difficult, this will **NOT** serve as a legitimate excuse for non-compliance. This legal uncertainty provides all the more reason for in-scope organizations to commence tackling ePrivacy compliance *sooner rather than later* – the *less* clear it is how the law will be applied, the more work organizations have to do to cover all primary risk bases. Particularly given that fines for non-compliance with ePrivacy mirror the astronomical fines set out in the GDPR.

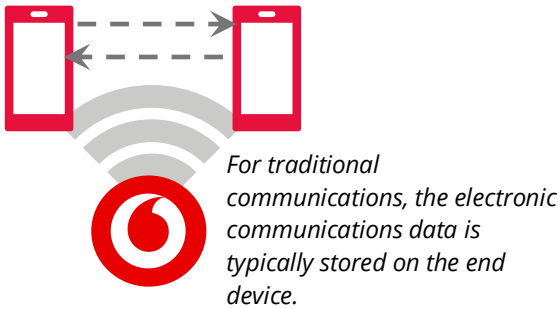
*With supervisory authorities across Europe already taking starkly different approaches to Cookies use under the GDPR, the MOST PRAGMATIC COMPLIANCE POSITION for organizations is to review the advice and enforcement cases on cookies use by their **local (or Lead) Supervisory Authority** and adapt controls according to their recommendations and decisions.*

[23] https://www.huntonprivacyblog.com/2018/11/21/uk-ico-issues-warning-washington-post-cookie-consent-practices/ (consulted 7 February 2019)

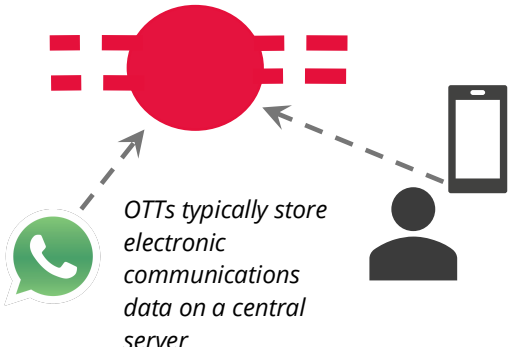
Protected in Transit only?

2002 ePrivacy Directive

The ePrivacy directive *already* makes provision to restrict interference with end-user's terminal equipment.[24] However, this could be more concretely composed to better enforce the right of individuals' to confidentiality of communications – in its current form the ePrivacy directive is **ambiguous** and there is scope for organizations (including information society services) to interfere with end-user's terminal equipment, provided the end-user is comprehensively notified and presented with the occasion to refuse the interference. This must be redrafted if individuals' rights of privacy and confidentiality are to be assured by European legislation.



For traditional communications, the electronic communications data is typically stored on the end device.



OTTs typically store electronic communications data on a central server

ePrivacy Regulation

However, the various incongruent drafts of the proposed ePR have only compounded this legal uncertainty: *whereas the text adopted by the European Parliament specifically amends the Commission proposal to ensure that electronic communications data is protected after it has been received, the Council text clarifies that the protection only applies in transit'.*[25]

Whilst it remains to be seen, it is perhaps more likely that the Parliament's version of the text will prevail over that of the Council. This is because the Council's stipulation that electronic communications data need only be protected in transit *fails* to capture the modern changes to messaging services, whereby electronic communication data is stored on a **central server**, as opposed to the ***device*** of the end-user (as is the case for traditional telecommunications providers). It is therefore Imperative that the ePR applies to communications data after receipt and not simply in transit. Indeed, were the Council's proposal to find its way into the final version, it would severely undermine the objective of updating data protection law to the 21st century. OTTs would continue to circumvent the strict requirements to which more traditional communication service providers are bound. It is important that Parliament and Council reach a consensus on this point, to

[24] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), *Official Journal L 201, 31/07/2002 P.0037 – 0047,* Article 5(3)

[25] https://edri.org/five-reasons-to-be-concerned-about-the-council-ePrivacy-draft/ (consulted 7 February 2019)

avoid further delay in the ePR and ensure continued protection of EU citizens by data protection legislation.

Internet of Things (IoT)

2002 ePrivacy Directive

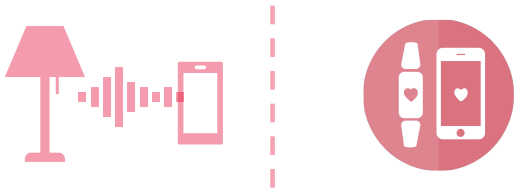
The 2002 ePrivacy directive covers services *'in public communications networks…including public communications networks supporting data collection and identification devices'*[26] In theory therefore, this should mean that all communication data – including machine to machine communication - is already in scope of ePrivacy rules, irrespective of the purposes and content[27].

ePrivacy Regulation

The Commission proposed in its 2017 draft of the ePR to include M2M transmissions within scope of the new legislation, in recognition of the technological advances which have led to machines using electronic communications networks in order to transmit information between them. However, problematically, the Commission's text *fails* to distinguish between those M2M communications containing **human information** (e.g. *smart watches*) and those that do not (e.g. air quality sensors). Consequently, the Commission's proposed ePR runs the risk of being overly restrictive and stifling innovation in the IoT sector.

In an attempt to liberalize these provisions, the Romanian Presidency has recommended that consent should not be required if the processing, storage and collection of information from end-users' terminal equipment *'is necessary for the provision of the information society services, such as those used by IoT devices (for instance, connected devices such as connected thermostats), requested by the end-user'.*[28]

Comparable?



***Undistinguished**: The Commission's ePR proposal would see smart watches and smart lights alike having to comply with ePrivacy rules*

However, the logic behind the Commission's overly restrictive provision is clear: to ensure that the new legislation remains effective in the face of further technological advances and that **privacy and security prevail** in an emerging IoT sector. It is for this same reason that the ePR, like the GDPR, is not prescriptive: it tells organizations what they have to do but does not prescribe how this must be done – to ensure that as technology evolves, it remains regulated by the new legislation.

Despite the seeming inconsistency between the overly-wide provision on M2M transmissions and the EU's values of business and innovation, it is more

[26] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), *Official Journal L 201, 31/07/2002 P.0037 – 0047,* Article 3

[27] Opinion 5/2016, Preliminary EDPS Opinion on the review of the ePrivacy Directive 2002/58/EC, 22 July 2016, section IV.2 pp.11

[28] Interinstitutional File 2017/0003(COD), 4 February 2019, pp.3

likely that the provision will remain wider in its application than be further narrowed. Whilst this of course depends, to some degree, on the effect of both lobbyists and parties contributing to the ePR (including all 28 Member States), traditionally European legislation sets a wider scope on its birth to ensure its relevance further into the future – and that is certainly one of the greatest challenges to any legislation aiming to govern the digital sector.

SECURITY REQUIREMENTS

SECURITY OF NETWORKS AND SERVICES

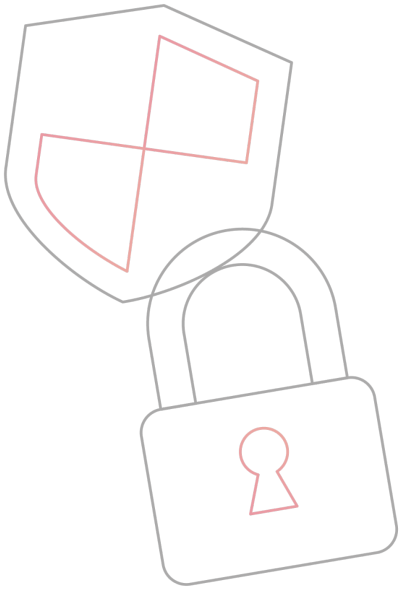
The provisions regarding the obligation of organizations to ensure security of their electronic communications networks and services using those networks remain *relatively unchanged* between the current ePrivacy directive and upcoming ePR. As with the GDPR, organizations are expected to implement both technical and organizational measures appropriate to the level of risk involved.[29] These provisions are unlikely to become overly specific in order to maintain a technology-neutral approach.

DATA BREACH NOTIFICATION

Similarly, the provisions on data breach notification in the proposed ePR have also not been significantly modified compared to the requirements of the current ePrivacy directive. However, further specification will be necessary to establish the interaction of the ePR rules on data breach reporting with those mandated by the GDPR. For example, were a data breach of personal data to arise in an electronic communications service, this could **trigger two different breach notification obligations** under both the GDPR and the ePR. With supervisory authorities across Europe having to re-resource to cope with

[29] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), *Official Journal L 201, 31/07/2002 P.0037 – 0047, Article 4* **and** Interinstitutional File 2017/0003(COD), Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), Recital 25

the elevated number of reported breaches post-GDPR, it would be inefficient to stipulate two sets of rules for data breaches as this would most likely double the number of notifications received by the regulators.[30] Further clarification is required as to the interaction of GDPR and ePR on data breach notification for it to remain an effective safeguard of individuals' rights and freedoms.



[30] Opinion 5/2016, Preliminary EDPS Opinion on the review of the ePrivacy Directive 2002/58/EC, 22 July 2016, section, VI.3, pp.12

TRAFFIC & LOCATION DATA

Telecommunications and Metadata

2002 ePrivacy Directive

Under current ePrivacy rules, organizations may only process electronic communications metadata for limited and specific purposes, outlined in the Directive, such as billing. This is in recognition of the fact that metadata tends to be more revealing than the content of the communication itself, such that it is *relatively easy* to draw **precise conclusions** about individuals' private lives if no restrictions are imposed on the processing of metadata.

ePrivacy Regulation

The draft version of the ePR proposes a liberalization of these provisions by permitting *further processing* of metadata for compatible purposes, **provided** that the data is first pseudonymized, not used for **profiling** individual users and *prior consultation* is sought with the relevant supervisory authority.

Despite the introduction of these aforementioned safeguards, the risk incurred by allowing further processing of metadata for compatible purposes would remain unmitigated. This is because what comprises 'compatible purposes' is **underdefined**, leaving service providers to determine what qualifies as compatible further processing.[31] Not only does this risk undermining standardization of ePrivacy rules from one service provider to another but, more importantly, it risks undermining the increased protection

[31] https://edri.org/five-reasons-to-be-concerned-about-the-council-ePrivacy-draft/ (consulted 12 February 2019)

conferred on end-users by the new data protection regime being advanced by the Commission.

To address this risk, the European Data Protection Board (hereinafter EDPB) have recommended that metadata can only be processed without the consent of the end-user if it has first been properly **anonymized**.[32] This would be a preferable solution compared with the pseudonymization route suggested by the earlier version of the ePR, as anonymization offers far greater security to the individual than does pseudonymization, from which an individual could still always be re-identified, with a little effort. Moreover, organizations who do anonymize the metadata would further benefit from the rules set out in the GDPR to the extent that any personal data elements revealed by the metadata, once anonymized, would fall out of scope of the GDPR and so could be legally used for further processing by the service provider.

Given that the provisions on metadata, alongside cookies, are some of the most contested elements of the proposed ePR, it would be wise for service providers caught by this requirement to commence **anonymizing** their **metadata** *as soon as possible*, as this is a widely-accepted security technique for reducing risk to data subjects/end-users and could **help off-set** the challenge of *complying with unclear legislation*.

[32] Statement of the EDPB on the revision of the ePrivacy Regulation and its impact on the protection of individuals with regard to the privacy and confidentiality of their communications; Section 1.

MORE RULES FOR MARKETING

SPAM

Marketing

2002 ePrivacy Directive

The directive currently in force allows organizations to send B2B electronic direct marketing **on an opt-out basis** and with no requirement for prior consent, depending, of course, on how this requirement has been implemented by the national authorities in each Member State. The rationale for this leniency was that this type of electronic marketing is conducted between companies and therefore incurred negligible risk to the rights and freedoms of individuals.

ePrivacy Regulation

However, just as the GDPR has elevated corporate email addresses to the status of personal data (in so far as they contain an individual's name), the draft ePR also proposes to align B2B direct marketing with the rules on B2C marketing, explicitly applying the provisions of the ePR to 'both natural and legal persons[33]. This means that organizations conducting B2B marketing would have to have **prior consent** of their corporate contacts *before* their details could be used for receipt of any marketing materials.

Practically speaking, this means that organizations purchasing lists of contact details from *third-party resellers* and **sales persons** using *apps* and *plugins* to scrape contact details

[33] Interinstitutional File 2017/0003(COD), Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), Recital 3

from online would have to review, and certainly **amend** (or potentially cease), such practices.

Finally, the ePR proposes that organizations seeking to conduct their marketing strategies over the phone will have to ensure their phone number appears on the call or indicate that the call is a marketing call by use of a designated pre-fix.

There is a common perception surrounding the new GDPR and ePrivacy regulation that these have been specifically designed to circumscribe the power of international conglomerates, such as Google and Facebook, who derive an entire economy from individuals' information. Whilst there is certainly some truth in this, that does not give cause to believe that all **non**-multinational conglomerates will avoid scrutiny and enforcement. It is worth noting the rapidly expanding market that is developing on the basis of surveillance and big data, as well as the number of start-ups and ad-tech[34] companies who all derive their business value from personal information. The ad-tech sector in particular should approach the ePrivacy regulation with as much *caution* as their multinational counterparts.

[34] https://martechtoday.com/as-gdpr-approaches-marketers-are-moving-away-from-their-reliance-on-third-party-data-215125 (consulted 11 February 2019)

DIRECTORIES & CALLING

PUBLIC DIRECTORIES

The new ePR appears to fortify the rules on public directories found in the current ePrivacy directive, such that consent must be collected from all end-users *before* their personal information can be included in a public directory. This is a **stricter** consent requirement that that set out in the ePrivacy directive, which only requires consent from the end-user where the purposes of the inclusion in the public directory are other than the search of contact details.

CALLING-LINE IDENTIFICATION

The requirement in the ePrivacy directive, that call recipients have a right to be informed as to the identification of a caller and take action against those who mask their caller ID, appears to have been maintained *relatively unchanged* in the proposed ePR.

NON COMPLIANCE MEANS BIG FINES

PENALTIES

Penalties for infraction are established in the 2002 ePrivacy directive *by reference to the Data Protection Directive* (hereinafter DPD). However, since the DPD has been repealed and replaced by the GDPR, this not only renders the DPD **obsolete**, but also has the effect of imposing the all new penalty scheme on the outdated ePrivacy directive.

This is problematic because there is deep legal uncertainty created by transposing penalties from a regulation to a *directive*. This is because regulations have direct effect and are automatically binding on all member states, whereas directives provide more leeway for member states to retain a degree of sovereignty in deciding how, and to what extent, the directive's requirements are implemented via national laws in their own country. Consequently, *penalties for ePrivacy non-compliance* have been awarded with **huge variation** across Europe. Forcing member states to align with a single penalty regime before there is legal impetus to do so (i.e. before the new ePrivacy regulation is adopted) undermines important legal concepts – such as hierarchy of norms – entirely.

CONCLUSION

Just as the GDPR is shrouded in legal uncertainty, so too is the new ePrivacy regulation. Uncertainty is typical of new legislation - not least because half of the authority on how to interpret and apply the rules of European law derives from case law. Legal uncertainty should provide **greater** (and not less) **Impetus** for organizations **to start tackling ePrivacy** compliance *as soon as possible*. Lack of certainty does not mean lack of enforcement. Lack of certainty means that the **business risk** faced by the organization in relation to the compliance objective is not sufficiently circumscribed, and therefore the overall compliance *risk increases*. This is particularly evident in light of the confused penalties rules, which makes it very difficult for organizations to know, not only how the proposed ePR will be enforced, but more importantly, how the rules of the *current* ePrivacy directive will be enforced, despite having set clear rules on this matter since 2002. This fact in itself should add greater urgency to the European Union's efforts to reach a consensus on the new ePR. In the meantime, it would be prudent that telecommunications - and especially OTT - providers start reviewing their treatment of electronic communications data as soon as possible to commence determining which processes are **likely to qualify as privacy intrusive** under the new regulation.

ABOUT THE AUTHORS

This White Paper was written by CRANIUM's ePrivacy expert team: Alexandra Calder (Privacy and Security consultant) and Maciej Skoniecza (Privacy and Data Protection consultant).

Alexandra first encountered ePrivacy working as a privacy consultant, assessing clients marketing approaches, which of course, today, are primarily adopted online. Recognizing the shortfall between the new GDPR and the outdated (but nevertheless, in force) ePrivacy Directive, Alexandra kept tabs on the ePrivacy Regulation's developments in hope of obtaining a concrete oversight to better direct compliance strategies. Unfortunately, no such overview appeared to exist and so together with her CRANIUM colleagues, Alex created exactly that.

*Maciej is CRANIUM's **ePrivacy expert** and is pivotal in ensuring CRANIUM remains at the forefront of developments in the data protection landscape. Maciej has followed the developments of the ePrivacy Regulation in detail (along with other European and International legislation governing the privacy and security of data), including attending live debates at the European Parliament and in-depth analysis of the various ePR drafts, European*

data protection decisions and cases and opinions and guidance of the European, independent and international bodies and authorities.

For more information and questions about our solutions contact: be-info@cranium.eu