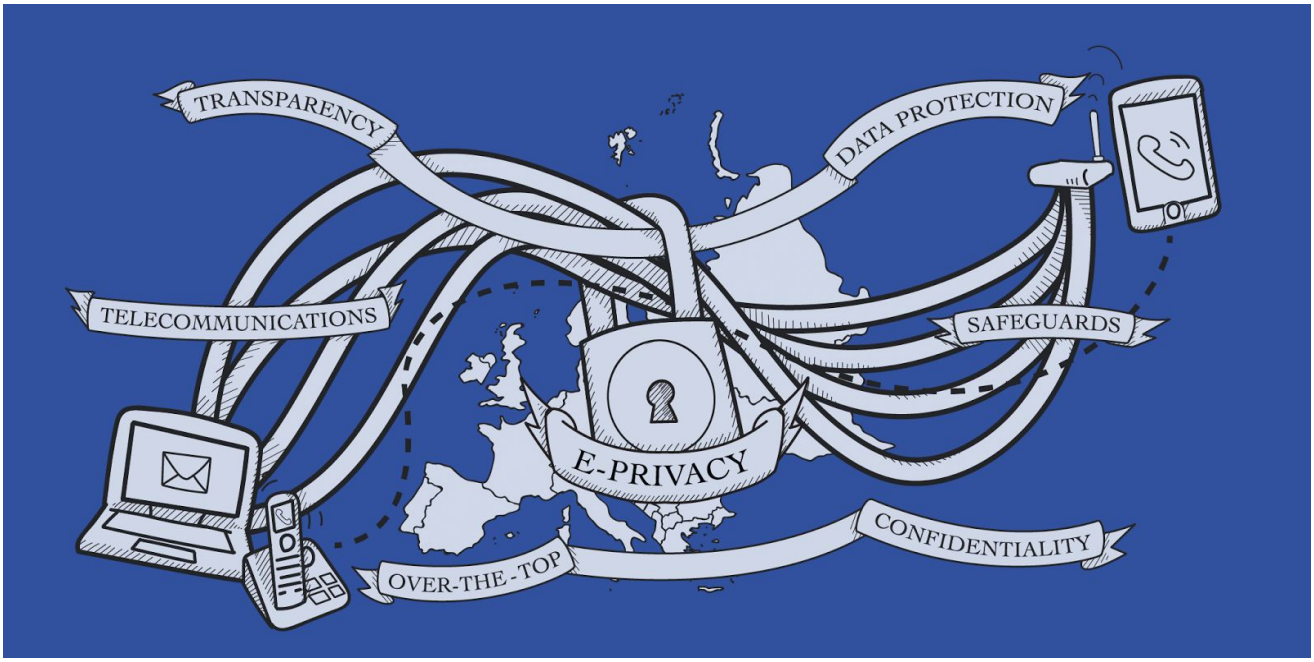
Review of the e-Privacy Directive



Executive Summary

The following paper provides an analysis of the e-Privacy Directive and its functioning over the past years. Access Now supports the development of an e-Privacy Regulation, a central piece of legislation for the development of a digital single market that would provide users with a high standard of privacy protection, help restore trust in businesses, and promote the use of tools to fight surveillance.

To achieve this goal, we make **ten specific recommendations** for lawmakers as the reform process of this legislation is taking place. These recommendations address core issues for the reform, such as the need for an e-Privacy framework; the expansion of scope; rules on data retention; tracking; confidentiality of communications; transparency reporting; encryption and privacy by design; the alignment with the General Data Protection Regulation; and the enforcement mechanism.

Table of contents

Introduction

Access Now is an international organisation that defends and extends the digital rights of users at risk around the world.[1] We are a team of 40, with local staff in 11 locations around the world. We maintain four legally incorporated entities - Belgium, Costa Rica, Tunisia, and the United States - with our tech, advocacy, policy, granting, and operations teams distributed across all regions. By combining innovative policy, user engagement, and direct technical support, we fight for open and secure communications for all.

We defend privacy globally. Access Now provided comments on the development and implementation of data protection and privacy rules in the Brazilian Marco Civil,[2] the African Union Convention on Cyber Security and Personal Data Protection[3], and the US Federal Communications Commission proposed broadband consumer privacy rules.[4] In the EU, we have been involved in the EU Data Protection Reform process since the tabling of the General Data Protection Regulation (GDPR) by the EU Commission in January 2012, and we have provided input to the Commission's public consultation of the review of the e-Privacy Directive.

In this paper, Access Now provides an analysis of the Directive concerning the processing of personal data and the protection of privacy in the electronic communications sector, also known as "e-Privacy Directive", ahead of its upcoming review by the EU legislators. In this paper, we provide recommendations to improve and strengthen the EU-wide rules on privacy and confidentiality of communications.

This paper is an update from our analysis dated July 2016, at a stage when the EU Commission had not yet introduced a legislative proposal, to reflect the current state of play in the debate on the reform. Our updates emphasise the scope of the future rules (in particular, the extension to "Over the Top" providers and information society services and the protections for content and metadata), the importance of consent, and the encryption debate. Our recommendations for this updated paper are based on the position paper we published in July 2016 and the extensive public discussion that has taken place since then. The Commission's new legislative proposal will be introduced in January 2017. [5]

[1] Access Now, https://www.accessnow.org/
[2] Access Now, Brazil must protect the Marco Civil regulatory decree, June 2016. https://www.accessnow.org/brazil-must-protect-marco-civil-regulatory-decree/
[3] Access Now, African Union adopts framework on cyber security and data protection, August 2014. https://www.accessnow.org/african-union-adopts-framework-on-cyber-security-and-data-protection/
[4] Access Now, Comments on the FCC Notice of Proposed Rulemaking on protecting the privacy of customers of broadband and others telecommunications services, May 2017. https://www.accessnow.org/cms/assets/uploads/2016/05/NPRM-PrivacyofBroadbandCustomers-_-Access-Now.pdf
[5] Access Now, Review of the e-Privacy Directive, July 2016. https://www.accessnow.org/cms/assets/uploads/2016/07/ePrivacy-Review-Policy-Paper-1.pdf

The need for an e-Privacy Regulation

1. Completing the EU data protection reform

The current e-Privacy Directive aims at **complementing and particularising** the Directive 95/46/EC on data protection. Similarly, the future framework will complete the recently adopted General Data Protection Regulation and provide protection for the right to private life as enshrined in Article 7 of the EU Charter of Fundamental Rights, which is not specifically covered by the scope of the GDPR. There is a need for specific protections to be articulated in the revision of the e-Privacy Directive.

In the spirit of the recently concluded EU Data Protection Reform, the current e-Privacy rules need to be modernised and upgraded to fit today's reality for the protection of privacy and confidentiality of communications. Since its adoption in 2002, the e-Privacy Directive has not successfully achieved its objectives, due chiefly to its failure to anticipate the rapid development of technology, as well as its fragmented implementation and weak enforcement.

The differences in the implementation of the rules by each member state have resulted in unequal protections and safeguards for users across the EU and an unnecessary complexity for cross-border businesses. Given these challenges, and for the sake of consistency, the e-Privacy legislation should be a Regulation. To provide the legal certainty and clarity needed by the private sector, and to protect users effectively, we must learn from the GDPR experience and refrain from adopting a "Regulective" - half Regulation, half Directive.

Aligning the e-Privacy reform with the GDPR will be crucial in order to avoid a conflict of laws, uncertainty for users' rights, and undue administrative burden for industry. For instance, the issue of data breach notification is sufficiently covered under the GDPR and need not be re-addressed under e-Privacy. The definitions for core concepts, such as consent, data minimisation, or purpose limitation, have been agreed under the GDPR and should be referenced, not redefined, in the e-Privacy legislation.

As *lex specialis*, the e-Privacy legislation must maintain and upgrade rules on confidentiality of electronic communications, traffic and data location, unsolicited communications, and itemised billing. New rules on tracking and mandatory transparency reporting should also be introduced and implemented. Overall, the future e-Privacy legislation should promote the development, spread, and use of technologies that protect the confidentiality of communications - both content and metadata - and safeguard user anonymity. To that end, legislators should refrain from establishing specific technical standards or requirements, as those could hinder security and create vulnerabilities that negatively impact users' rights and ultimately undermine the objective of the e-Privacy legislation.

2. Trust

Security and privacy are crucial to ensure trust in the digital economy and the digital single market, which in turn is key for business development, revenues, and growth. Improving security

for users when surfing the web and ensuring digital privacy are in general high on the European Commission's list of priorities. The e-Privacy Directive is a key instrument to achieve these objectives.

At a time when smartphones are an increasingly predominant support for communication, developers are creating new applications, and companies are rolling out a plethora of connected products, it has never been more relevant and necessary to ensure a high level of protection for privacy and confidentiality of communications through the e-Privacy Directive.

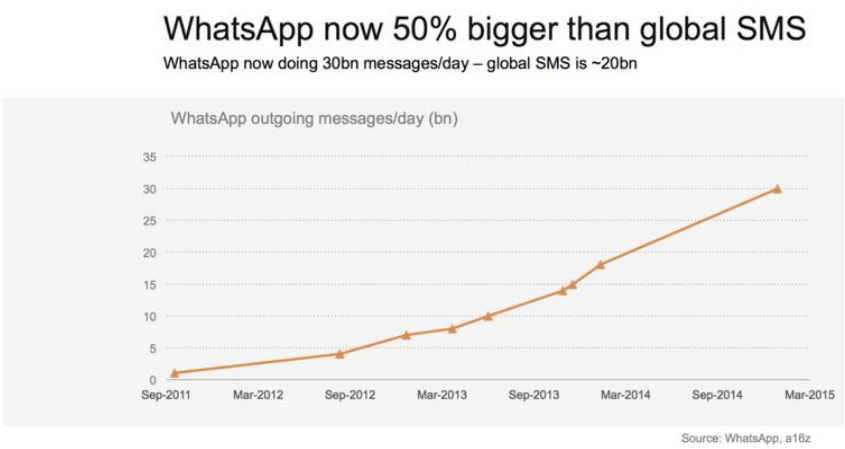
During the upcoming reform process, lawmakers will be tasked with developing measures that anticipate how future developments related to online tracking and marketing or behavioural advertising will impact users' privacy and the confidentiality of our communications. To do so, while avoiding creating burdens for users and businesses, law makers must develop measures for a future e-Privacy Regulation that are technologically neutral and focused on addressing the impact of privacy-intrusive technologies, rather than regulating or prescribing the development of specific applications.

Scope of the future Regulation

1. Extension to "Over the Top" services and information society services

When the e-Privacy Directive was adopted in 2002, legislators were unable to sufficiently anticipate the impact that smartphone applications, online tracking, javascript, social media services, or behavioural advertising would have on internet users' right to privacy and confidentiality of communications. As the EU Commission, the Parliament, and the Council of the EU work to modernise and upgrade the current rules, the scope of the e-Privacy legislation should be broadened to cover not only telecoms operators but also the so-called Over the Top (OTT) communications services and, more broadly, information society services.

Today, communication does not take place only through services provided by telecoms operators, but also through similar services and applications offered by online services such as Line, Whatsapp, Skype, Google Hangout, Slack, or Signal. In the past few years, OTT communications services and information society services have overtaken traditional communications platforms such as phone and SMS, with more messaging being sent via these modern services. Furthermore, studies have found that while services like Whatsapp - which



have an estimated 800 million active users and can handle more than 30 billion messages a day - continue to gain popularity, the volume of messages sent via SMS has declined globally.[6] Since users increasingly rely on OTT services and information society services to communicate, we must apply privacy rules that ensure the confidentiality of their communications to the sector.

2. Interaction with the Telecoms Package

Both telecoms operators and communications platforms should abide by privacy and data protection rules; telecoms-style licensing should however be limited to traditional operators. Internet services and applications should not be subject to licensing requirements or pre-government authorisations that are specific to the telecom or broadcast sector, as this would harm free expression, access to information and, the open internet. Therefore, while OTT should be covered by the e-Privacy Directive, those services should not be included in the scope of the licensing provisions of the Telecoms package reform.

Confidentiality of electronic communications

1. Users' consent

The future e-Privacy Regulation should include a positive obligation for providers of electronic communications, including providers of OTT services, to protect users' anonymity and the confidentiality of their electronic communications - both content and metadata - thus reaffirming the objective of this legislative instrument. More specifically, the current rules on traffic and data location, unsolicited communications, and itemised billing must be maintained and upgraded.

To complement communications services' obligation to protect rights, users' explicit consent must be requested for the processing of information that falls within the scope of the e-Privacy Directive. It is imperative to ensure control over access to and processing of the extremely personal information of our daily communications that take place over the phone, messaging apps, or the web. Both the metadata and the content of these communications can reveal highly sensitive information about users, and this information must therefore be protected with the highest legal standard for processing: the user must give explicit consent, which must be informed, affirmative, and specific to a clearly defined purpose. Explicit consent will give users the appropriate level of control of their information, as well as predictability. If companies would be authorised to process users' information without their knowledge through a "legitimate interest" clause, users would be stripped of control over their own information as they would not know who is using their information and why.

Therefore, the new e-Privacy Regulation should not allow for a derogation from the privacy requirements in the form of a "legitimate interest" exception.

[6] Ofcom, International Communications Market Report, December 2014. http://stakeholders.ofcom.org.uk/binaries/research/cmr/cmr14/icmr/ICMR_2014.pdf

2. Traffic and location data & terminal equipment

The protection of user metadata has often been overlooked and its impact on privacy downplayed. However, in recent years, its relevance has been clearly established. Studies indicate that metadata is just as revealing as the content of communications itself.[7] The Dutch NGO Bits of Freedom conducted research and published a comprehensive report on how much metadata information gathered by mobile companies on browsing activities or users' movements reveals about the user and the people with whom the individual is communicating.[8] By collecting a user's metadata over a single week, researchers were able to find out the user's age, religion, address, and partner's name and occupation. They were even able to guess the user's password from analysing search results and music preferences. The importance of metadata was further demonstrated through a study run by the Swiss civil society group Digitale Gesellschaft Switzerland during a campaign on data retention. The group produced a visualisation of six months' worth of metadata from one of the members of the Swiss national parliament, Balthasar Glättli, with his consent.[9] With these data, they created an image of M. Glättli's life drawn from information about his use of social media, as well as his movements. They were able to establish where M. Glättli lives, when he goes to sleep, when he goes work, whom he is meeting, with whom he regularly communicates, how many emails he sends and receives per day, and how much he has travelled, at what speed.

Stewart Baker, former general counsel of the United States National Security Agency (NSA), confirmed the relevance of metadata when he declared, "metadata absolutely tells you everything about somebody's life. If you have enough metadata, you don't really need content." [10] Michael Hayden, former director of the NSA and the Central Intelligence Agency, reinforced this point when he explicitly stated, "we kill people based on metadata."[11]

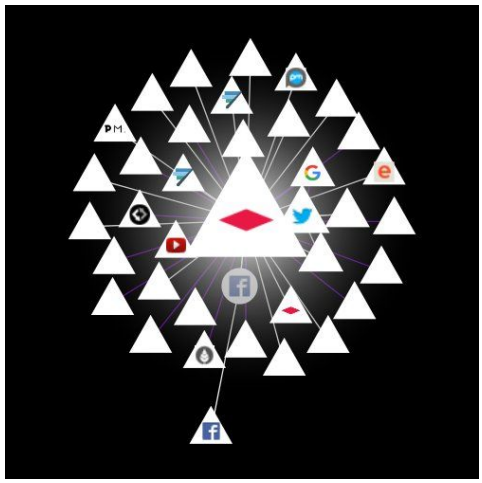
Since metadata is relevant, it must be included in the new e-Privacy rules, and not just traffic and location indicators. In addition, we must clarify the rules on the use and reuse of metadata. Currently, the e-Privacy Directive authorises the use of traffic or location data if it is for a clear purpose, if the user has given his or her consent, and if the information will be anonymised. The Open Rights Group, the UK-based NGO, recently published a report on how phone companies use personal data which addresses the caveats for anonymised data under the e-Privacy Directive.[12] Findings indicate that in the UK, implementing the e-Privacy Directive's provision on data anonymisation has not provided sufficient safeguards for users, as in many cases personal attributes such as names were replaced by a code that still enabled identification of individual

[7] Jonathan Mayer, Patrick Mutchler, and John C. Mitchell, Evaluating the privacy properties of telephone metadata, March 2016. http://www.pnas.org/content/113/20/5536.full
[8] Bits of Freedom, How your innocent smartphone passes on almost your entire life to the secret service, July 2014. http://www.statewatch.org/news/2014/jul/bits-of-freedom-on-the-metadata-of-your-phone.pdf
[9] Digitale Gesellschaft Switzerland, Data retention in Switzerland - The monitored life of National Councilor Balthasar Glättli, May 2014. https://www.digitale-gesellschaft.ch/dr.html
[10] Alan Rusbridger, The Snowden Leaks and the Public, The New York Review of Books, November 2013. http://www.nybooks.com/articles/2013/11/21/snowden-leaks-and-public/
[11] Johns Hopkins University, The Price of Privacy: Re-Evaluating the NSA, April 2014. https://www.youtube.com/watch?v=kV2HDM86XgI
[12] Open Rights Group, Cashing in on your mobile? How phone companies are exploiting their customers' data, 2016. https://www.openrightsgroup.org/assets/files/pdfs/reports/mobile-report-2016.pdf

users. Due to these shortcomings, the processing of metadata, including traffic and location data, should always be contingent on the user's consent. Exceptions can be made for billing and interconnection payments where processing for these specific purposes can be authorised through explicit mention in the user's contract, and if the processing lasts only for the period during which the bill may be lawfully challenged.

3. Tracking

The 2015 EuroBarometer survey indicated that tracking is a major source of concerns for European users.[13] Respondents were particularly concerned about their everyday activities being recorded via providers of mobile phone networks or applications, the recording of everyday activities on the internet, and the tracking of their behaviour via payment cards. Access Now has first-hand insight into the privacy implications of tracking and the increased use of identifiers. In October 2014, Access Now launched the AmIBeingTracked.com initiative to enable users of mobile internet access services to determine wheter their internet service provider was using "supercookies" - special tracking headers that the telecoms providers inject beyond the control of the user.[14] Since its launch in October 2014, more than 330,000 people used the tool, and the results showed significant and secret global deployment of supercookies. We have conducted tests in 10 countries, two of which are EU member states: Spain and the Netherlands. We found that at least two providers in Spain and the Netherlands used supercookies without notifying the affected users. We also found that the use of the "Do not track" tools in web browsers did not block or prevent the tracking headers injected by the telcos in question.



Current rules within the e-Privacy Directive fail to distinguish between different types of online tracking, and enforcement has largely focused on the use of cookies. Current practices indicate that tracking goes far beyond cookies and can happen across websites, applications, and even devices. These shortcomings should be addressed in the future review and focus on creating technologically neutral obligations and safeguards around the use of tracking tools and techniques in general, rather than targeting a specific technology.

Clear distinctions should be made between technical mechanisms that are used to facilitate the mere functioning of websites and online services and those which are used for the purpose of mapping and analysing a user's behaviour. The more privacy-invasive the tracking, the stricter the user protections should be. There are different types of tracking, including first-party or third-party hosted, and their impact on privacy varies extensively. Most of these distinctions are not made transparent to users. For instance, the above image illustrates the number of third party instruments which track any user who enters a simple newspaper webpage; in this case

[13] European Commission, Special Eurobarometer on Data Protection, March 2015. http://ec.europa.eu/public_opinion/archives/ebs/ebs_431_en.pdf

[14] Access Now, The Rise of Mobile Tracking Headers: How Telcos Around the World Are Threatening Your Privacy, August 2015. https://www.accessnow.org/cms/assets/uploads/archive/AIBT-Report.pdf

Libération. Users should be informed about the most invasive types of tracking such as identifiers placed or collected by a third party for behavioural advertising purposes and identifiers used for frequency capping.

Lastly, while the establishment of profiles and effects of profiling are partially addressed by articles 21 and 22 of the GDPR, on the right to object and on automated decision-making, respectively, further provisions to complement and particularise those rules should be developed in the e-Privacy Regulation to prevent the creation of profiles on the basis of information collected through tracking mechanisms.

Data retention

Article 23 of the GDPR covers the content of Article 15 of the e-Privacy Directive, which includes a provision authorising the use of data retention schemes. This Article should be removed from the update as it is redundant with Article 23 in the GDPR. Member states have taken advantage of the current uncertainty under EU law to enact data retention mandates which have a deleterious impact on human rights, the environment, and the digital economy. The retention of vast amount of data requires massive storage capacity, cooling systems, security protections, and more. The costs of data retention have been demonstrated, and highlighted in the EU Commission evaluation report on the Data Retention Directive, but the necessity and proportionality of such measures on the protection of user data has yet to be assessed and duly demonstrated.[15] On the contrary, the Court of Justice of the EU has established in Joined Cases C-293/12 and C-594/12 that data retention schemes have a severe impact on the user's right to privacy.[16]

Encryption and government access to personal data

Over the past few months, some stakeholders have repeatedly indicated that the e-Privacy Directive could be used to undermine encryption, even if the nature of this Directive is antithetical to this approach. We acknowledge that there are risks that the legislation could be weakened during the reform process, given that some member states are pushing for circumvention of encryption, and industry has continually attacked the ePrivacy Directive as a whole.

However, regardless of the e-Privacy Directive review process, states are currently pushing for a way to circumvent encryption, either through exploiting vulnerabilities or through hacking. You can see this illustrated by the recent court ruling in Belgium's town of Mechelen regarding

[15] European Commission, Evaluation report on the Data Retention Directive 2006/24/EC, April 2011. https://www.eff.org/files/filenode/dataretention/20110418_data_retention_evaluation_en_0.pdf

[16] Court of Justice of the EU, Joined Cases C-293/12 and C-594/12 Digital Rights Ireland and Seitlinger and Others, April 2014. http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d0f130d55d08eb1720de47b5a541d28dd15fb049.e34KaxiLc3eQc40LaxqMbN4Pa3aPe0?text=&docid=150642&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=586215

access to Skype customer data, the data retention mandates, and the inclusion of hacking powers in the United Kingdom's Investigatory Power Act.[17] The e-Privacy Directive is the best instrument to help businesses resist the pressure of developments like these, protect their products and infrastructure, and shield their users from privacy violations. The Directive promotes and protects the confidentiality of communications. Privacy-by-design tools, such as encryption, are specifically mentioned in the current Directive as ways to guarantee this right. By extending the scope of the future e-Privacy Regulation, increasing the promotion of privacy-by-design tools, and promulgating rules on confidentiality of communications, we have the opportunity to make products and services more resilient, help protect users against surveillance, and push back on the technical level against state's desire to undermine products. The e-Privacy legislation is also the right tool to re-establish user trust.

To further advance safeguards for the confidentiality of communications - both content and metadata - the future e-Privacy Regulation should promote the general use of privacy-enhancing technologies as well as tools which protect users' anonymity. Those rules must be technologically neutral and not request the industry or users to use a specific standards, as such criteria would make it easier for external actors to undermine the selected tools and trump their potential benefits. To that end, legislators should not erode the security of devices or applications, either by introducing a legal requirement for vulnerabilities or by mandating backdoors into products or services. They should not pressure companies into keeping private data, allow law enforcement to access to it, or retain encryption keys to decrypt the data.[18] Echoing the United Nations 2016 resolution on privacy, we calls upon governments to "refrain from requiring business enterprises to take steps that interfere with the right to privacy."[19] The UN also encourages companies "to work towards enabling secure communication and the protection of individual users against arbitrary or unlawful interference of their privacy, including by developing technical solutions." This timely resolution strikes significant parallels with the objectives of the e-Privacy review.

In short, it is a mischaracterisation of the legal environment to suggest that the new e-Privacy rules, and the extension of the scope to OTTs, will lead to legislative action from member states to introduce new powers for government access to data. Member states' surveillance of, and unlawful access to, personal data pose serious risks for the rights to privacy and data protection. Legislators must make sure not to open new windows within the e-Privacy for such measures. In a letter sent to the Council Presidency, the French and German Interior Ministry called for "reinforcing the legal obligation of electronic communications providers to cooperate with law enforcement authorities".[20] We recognise the need for member states to ensure the security of people living the EU; this goal can only be achieved if the foreseen cooperation with

[17] Techdirt, Belgian Court Fines Microsoft For Failing To Comply With Its Impossible Order, 2016. https://www.techdirt.com/articles/20161030/06444835913/belgian-court-fines-microsoft-failing-to-comply-with-impossible-order.shtml and United Kingdom, Investigatory Powers Act 2016. http://www.legislation.gov.uk/ukpga/2016/25/contents/enacted/data.htm

[18] Global open letter encouraging international leader to support the safety and security of users, companies, and governments, 2016. https://www.securetheinternet.org/

[19] United Nations, General Assembly, The right to privacy in the digital age, 2016. https://www.accessnow.org/cms/assets/uploads/2016/09/privacy-resolution-2016-UNGA.pdf

[20] Council of the European Union, German-French letter concerning cooperation between law enforcement agencies and electronic communication service providers, 2016. http://data.consilium.europa.eu/doc/document/ST-14001-2016-INIT/en/pdf

providers of electronic communications does not lead to the establishment of vulnerabilities in networks or devices, and if we prevent unlawful access to information. Such measures would put all users at risks. There is no secure way to provide authorities with a "magic key" or other form of exceptional access. Any deliberate vulnerabilities or backdoors in our technology would inevitably pave the way for exploitation. Any attempt to undermine the development or use of encryption or other tools and technologies to protect the confidentiality of communication would also undermine the fundamental right to privacy as well as the integrity of our systems, and therefore stands at odds with the objective of the e-Privacy legislation. It is important to note that regardless of the member states' competence under the public security exemption, the requirements for proportionality and necessity under the EU Charter for Fundamental Rights still apply. Access Now is keen to challenge laws and policies that violate the right to privacy, in collaboration with other stakeholders

Transparency reporting

The review of the e-Privacy legislation is a unique opportunity to introduce into law a mandatory requirement for transparency reporting. Transparency reporting is a pathway for technology companies to disclose threats to users' privacy and freedom of expression. Such reports educate the public about enforcement of company policies and safeguards against government abuses, and contribute to an understanding of the scope and scale of online surveillance, internet shutdowns, content restrictions, and a host of other practices that impact users' fundamental rights.

To date, at least 61 companies worldwide have released transparency reports on a voluntary basis.[21] A clear reporting obligation[22] would extend this best practice to every communications provider in the EU - both telecoms operators and OTTs - and harmonise the content of such reports by providing clear guidance on the information that must be included. We recommend that at minimum the reports include statistics and information on government and third-party requests for access to user data, on takedown or restriction of content or accounts, and on network disruptions, along with clear explanation of corporate processes and policies responding to these requests and incidents.[23]

Competent authorities

Enforcement of the future e-Privacy Regulation should be assigned to the Data Protection Authorities (DPAs), who have expertise in this area, and not to telecoms regulators, as is so often

[21] Access Now, Transparency Reporting Index. https://www.accessnow.org/transparency-reporting-index/
[22] While we do not fully endorse its guidelines, the Canadian Government's Industry Canada has published a set of voluntary standards it recommends businesses follow in transparency reporting: Government of Canada, Transparency reporting guidelines, June 2015. http://www.ic.gc.ca/eic/site/smt-gst.nsf/eng/sf11057.html
[23] More expansive reporting best practices can be found at (currently being updated): Ranking Digital Rights, Corporate Accountability Index criteria, July 2016.
https://rankingdigitalrights.org/2016/07/05/new-draft-methodology

the case. This will facilitate uniformity across sectors, as DPAs are already tasked with enforcing the GDPR.

Furthermore, while the implementation of a single set of rules agreed under a Regulation will facilitate harmonised enforcement and help users seek redress of privacy violations, further safeguards for an efficient right to remedy must also be put in place. Specifically, the future e-Privacy Regulation should apply the “cooperation and consistency” enforcement mechanism agreed upon under the GDPR and similar administrative fines should be developed within the e-Privacy Regulation.

Finally, the 2015 EuroBarometer indicates that only 37% of the respondents are aware of the existence of data protection authorities and even those respondents broadly do not know how to seek assistance and redress. To improve users’ access to remedy, the e-Privacy Regulation should clearly authorise consumers and non-for-profit organisations to represent a user or a group of users in claims in front of supervisory authorities. To ensure meaningful access to remedy, the legislation should also make clear that participation in administrative enforcement mechanisms do not preclude or prevent users from seeking judicial remedy.

Conclusion & recommendations

Access Now supports the EU Commission's efforts in the reform of the e-Privacy Directive and looks forward to engaging with the legislators and all stakeholders to achieve a high-level of protection for users' right to privacy and confidentiality of communications. To that end and to support the analysis provided in this paper, we have developed the following list of recommendations.

1. The future e-Privacy piece of legislation should be a **Regulation**.

2. Measures on data breaches and the compliance and enforcement mechanism should be **aligned with the GDPR.** Specifically, compliance and oversight of the e-Privacy Regulation should be the task of data protection authorities. Their enforcement power should include administrative fines for repeated failures to comply with the e-Privacy rules.

3. The **scope** of the e-Privacy Regulation should include telecoms operators, **OTT communications services, and information society services**.

4. Users' **explicit consent** must be requested for the processing of their information.

5. **Increased protection for metadata** must be included.

6. Rules on **tracking** must be extended and made **technologically neutral**.

7. **Article 15 of the e-Privacy Directive must be removed**.

8. Increased **promotion and general rules on the protection of privacy by design tools** and techniques such as encryption should be added. Those rules must be technologically neutral and not request the industry or users to use specific standards. The new e-Privacy Regulation must contain rules that protects the right to privacy of users from member states to avoid the creation of loopholes for government access to data related to either telecoms operators, OTTs, or information society services.

9. The e-Privacy Regulation should include a measure on **mandatory transparency reporting** with a clear set of criteria.

10. Rules on **collective redress mechanism,** and **representation rights** for non-for-profit organisations on behalf of users in claims, should be developed.

For More Information
Please visit www.accessnow.org

Contact
Estelle Massé | Senior Policy Analyst | estelle@accessnow.org