Review of the e-Privacy Directive

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 10 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.

The need for an e-Privacy Regulation

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.

[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

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, partially due to its fragmented implementation, weak enforcement and chiefly, due to its failure to anticipate the rapid development of technology.

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 future e-Privacy should be a Regulation. In order to provide the legal certainty and clarity needed by the private sector, and to be effective at protecting users, we need to 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 an unduly administrative burden for the industry. For instance, the issue of data breach notification is sufficiently covered under the GDPR and need not be re-addressed under e-Privacy. More to the point, all definitions of core concepts, such as consent, data minimisation or purpose limitation, agreed under the GDPR should be referenced into the future e-Privacy legislation.

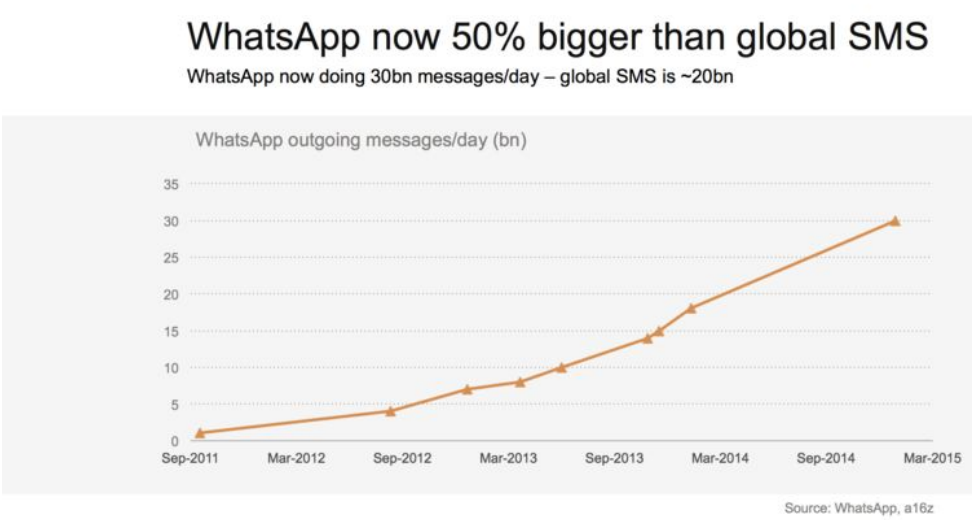
As *lex specialis*, the e-Privacy must maintain and upgrade rules on confidentiality of electronic communications, traffic and data location, unsolicited communications, and itemised billing. New rules on tracking and mandatory transparency reporting should also be introduced and implemented. Overall, 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, the 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.

Scope of the future Regulation

At the time of the adoption of the 2002 e-Privacy Directive, legislators were not able to sufficiently anticipate the impact which 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, Parliament and Council of the EU work to modernise and upgrade the current rules, the scope of the e-Privacy should be broadened to cover not only telecoms operators but also the so-called Over the Top (OTT) providers.

Today, communication does not only take place over 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, traditional communications

platforms such as phone and SMS have been overtaken by OTTs communications services, with more messaging being sent through their modern services. To further the point, studies have found that while services like Whatsapp - which count 800 million active users and handle more than 30 billion messages a day - continue growing, SMS volumes have declined all over the world.[5] Over the Top messaging applications seem to be replacing traditional SMS services. As users increasingly rely on OTT services and applications to communicate, privacy rules ensuring the confidentiality of communications need to apply to this sector too. The revised e-Privacy legislation should also clarify that its obligations apply to both the provision of publicly available electronic communications services in public and publicly accessible private communications networks in the Union to ensure harmonised users' rights and reduce complexity in the implementation of the law.



Confidentiality of electronic communications

1. Positive obligation, traffic and location data & terminal equipment

The future e-Privacy Regulation should include a positive obligations for providers of electronic communications, including providers of OTT services, to protect users' anonymity and 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.

The protection of user metadata has often been overlooked and its impact on privacy minimised. However, in recent years, its relevance has been clearly established. Studies indicate that metadata is just as revealing as the content of communications itself.[6] 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 user movements reveals

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

about the user and the people with whom they are communicating.[7] 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 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 where they produced a visualisation of six months worth of metadata of one of the members of the Swiss national parliament Balthasar Glättli, with his consent.[8] With this data, they were about to build a visual profile providing an a image of the M. Glättli's life by monitoring his social media usage and analysing his movements. They were able to establish where M. Glättli lives, when he goes to sleep, when he goes work, whom he is meeting, and with whom he regularly communicates, how many emails he sends and receives per day, how much he has travelled and at what speed.

The relevance of metadata has been confirmed by former General Counsel of the United States National Security Agency (NSA) Stewart Baker who declared, "metadata absolutely tells you everything about somebody's life. If you have enough metadata, you don't really need content."[9] This was furthered by former director of the NSA and the Central Intelligence Agency General Michael Hayden when he indicated, "we kill people based on metadata."[10]

Given their relevance, the protection of metadata, beyond just traffic and location indicators, must be included. In addition, rules on the use and reuse of metadata must be clarified. Currently, the use traffic or location data is authorised under the e-Privacy Directive, if it is for a clear purpose and if the user has given his or her consent or if the data is being anonymised. The UK based NGO, Open Rights Group, has recently published a report on the use of personal data by phone companies which addresses the caveats for anonymised data under the e-Privacy Directive.[11] Findings indicate that the implementation of the e-Privacy Directive provision on data anonymisation in the UK has not provided sufficient safeguards for users, as in many cases personal attributes such as names were replaced by a code which still enabled identification of individual 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 this specific purposes can be authorised if explicitly mentioned in the user's contract and if the processing lasts only for the period during which the bill may be lawfully challenged.

---

[7] 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

[8] Digitale Gesellschaft Switzerland, Data retention in Switzerland - The monitored life of National Councilor Balthasar Glättli, May 2014. https://www.digitale-gesellschaft.ch/dr.html

[9] 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/

[10] Johns Hopkins University, The Price of Privacy: Re-Evaluating the NSA, April 2014. https://www.youtube.com/watch?v=kV2HDM86XgI

[11] 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

Finally, to further advance safeguards for the confidentiality of communications - both content and metadata - the future e-Privacy Regulation should promote the use of privacy-enhancing technologies as well as tools which protect users' anonymity. To that end legislators should not erode the security of devices or applications by either introducing a legal requirement for vulnerabilities or backdoors into products or service or by pressuring companies to keep and allow law enforcement access to data, or have access to the encryption keys to private data.[12] There are no secure methods to provide for a secure "magic key" or other form of exceptional access. Any vulnerabilities or backdoors would inevitably pave the way for exploitation. Any attempt to undermine the development or use of encryption or other tools and technologies protecting the confidentiality of communication would also undermine the fundamental right to privacy as well as the integrity of communications and systems, and therefore stands at odds with the objective of the e-Privacy legislation.

2. Tracking

The 2015 EuroBarometer survey indicated that tracking is a major source of concerns for 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 increase use of identifiers. In October 2014, Access Now launched AmIBeingTracked.com 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, 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 those EU countries used supercookies, without notifying 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.

Current rules under the e-Privacy Directive fail to distinguish between different types of online tracking and enforcement has largely focused on the use of cookies, specifically. Current practices indicates 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 obligations and safeguards around the use of tracking tools and techniques in general, rather than targeting a specific technology.

---

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

[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

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. For instance, 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. The more privacy-invasive the tracking, the stricter the user protections should be. While the establishment of profiles is partially addressed by articles 21 and 22 of the GDPR, respectively on the right to object and on automated decision-making, further provisions to complement and particularise those rules should be developed in the e-Privacy Regulation. 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.

Data retention

Article 23 of the GDPR covers the content of Article 15 of the e-Privacy Directive, which include a provision authorising the use of data retention schemes. This Article should be removed as it is now redundant. 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]

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 one of the strongest ways for technology companies to disclose threats to user 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 impacting users' fundamental rights.

---

[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

To date, at least 61 companies worldwide have released transparency reports on a voluntary basis.[17] A clear reporting obligation[18] would extend this best practice to every communication provider in the EU - both telecoms operators and OTTs - and harmonise the content of such reports by providing clear guidance on the minimum information that must be included. At minimum, we recommend 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.[19]

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

Furthermore, while 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.

For More Information
Please visit www.accessnow.org

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

[17] Access Now, Transparency Reporting Index. https://www.accessnow.org/transparency-reporting-index/
[18] 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
[19] 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