Track or be tracked? The challenges of the ePrivacy Regulation

Check this presentation at: https://edri.org/diego/

Diego Naranjo – Senior Policy Advisor
@DNBSevilla  diego.naranjo@edri.org
European Digital Rights (EDRi) is an association of civil and human rights organisations from across Europe. We defend rights and freedoms in the digital environment.
(some) Human Rights frameworks

UN Declaration of human rights:

- Article 12: No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.

EU Charter of Fundamental Rights

- Article 7: Respect for private and family life
- Article 8: Protection of personal data
EU Rules on Data Protection & Privacy

Existing:


To be replaced respectively by

- General Data Protection Regulation – GDPR (passed in 2016, in force from May 2018)
- New “Police Directive” (passed in 2016, in force from May 2018)
- ePrivacy Regulation (ongoing, expected for 2018)
future ePrivacy Regulation
The e-Privacy Directive was created to complement the Data Protection Directive.

It covers **specifically** privacy, confidentiality of communications and data protection issues in the electronic communications sector.

The proposal is a good step forward but it has been watered down after the leak of the text in December.

Civil society and industry lobbyists are already in passionate discussions about the text: “End of the Internet as we know it!”
• **Telecoms, Online advertisers, Publishers:** “We don’t need more regulation, we need to use Big Data and profiling to create jobs and innovation”

• **Some policy makers** “We like innovation and data flows and stuff!!!!”

• **European Commission:** “We understand we need to protect privacy and confidentiality of communications. Help us out!”
EDRi thinks that...

- We need ePrivacy to complement the GDPR in the era of the Internet of Things, massive surveillance and more and more e-communications
- It needs to be harmonised across the EU
- It is not about annoying cookie notices, it is about privacy and confidentiality of communications
- Some telecoms just want to profile citizens to compete with other Big Data businesses
- Watchout: Governments ❤️ Backdoors (ie: exceptions for “national security”
ePrivacy

EDRi thinks that...

- We need ePrivacy to complement the GDPR in the era of the Internet of Things, massive surveillance and more and more e-communications
- It needs to be harmonised across the EU
- It is not about annoying cookie notices, it is about privacy and confidentiality of communications
- Some telecoms just want to profile citizens to compete with other Big Data businesses
- Watchout: Governments Backdoors (ie: exceptions for “national security”)

on the proposal of an e-Privacy Regulation
ePrivacy

and specifically...

• **Trust is needed**: NTIA report showed that 45% of households had refrained from certain online activities in the previous year, due to privacy and security fears

• **Broadening of the scope** to other new actors, such as OTTs (Skype, Whatsapp as common methods of communications)

• Keep the focus on **tracking**, rather than on specific tools (cookies, device fingerprinting)

• We need a **ban on “cookie walls”** for private and public websites

• **Privacy by default**, not “privacy by option”

• **Collective redress** needs to be ensured
Blurry issues:

- Article from the ePR allowing data retention laws: repeal or clarify?
- OTTs using end-to-end encryption in apps: Is it dangerous or positive for privacy to include them in the new ePR?
- Alternatives to "free" services if people don't want to pay for them (as EU research shows)
- Encryption backdoors and "needed access" for law enforcement purposes
Questions, comments? 
@DNBSevilla
@edri

diego.naranjo@edri.org