PROGRAMME

Track 01 re-imagining the digital public sphere
Topics: #uploadfilters #censorship #algorithms #automation #fakenews #hackingelections #filterbubbles #propaganda

Track 02 [in]security of devices
Topics: #statehacking #encryption #surveillance #statemalware #E-evidence #security

The first track will focus on the challenging dynamics that we have been facing as we imagine a democratic digital public sphere. The topics covered will include the privacy-invasive measures to censor legitimate speech online as well as the role that algorithms play in curation and governance with sessions on algorithmic decision-making, accountability, fake news and the spread of propaganda.

The second track will include sessions on state hacking and malware, law enforcement access to user data (so-called "e-evidence") and device security. It will also include hands-on tutorials on how to protect your communications better.

Time	Auditorium 3	Auditorium 4	Foyer
09:30-10:00			*Coffee*
10:00-10:15	Welcome (Imge Ozcan, Rocco Bellanova, Kirsten Fiedler)		
10:30-12:00	10:30-12:00 Salle du Conseil (4th floor): EDPS-CSO summit		
	Digital Privacy – low and high hanging fruits, and how to pick them	Work & Networking space	
12:00-13:00			*Lunch break*
13:00-14:30	Round-table: Government hacking in different national contexts & strategies for challenging surveillance	From "old" filter bubbles to political microtargeting	
14:30-14:45			*Coffee break*
14:45-16:00	Government hacking: Exchange with policy-makers	Investigating algorithmic systems: Algorithm auditing	Open Internet Privacy Bar (14.30-15.30) Privacy and security in the blender: How to better protect your digital life (offered by Privacy Training Center); Q&A
16:00-16:15			*Coffee break*
16:15-17:45	The use of AI by public authorities	Strip searching the internet	Open Internet Privacy Bar (16.30-17.30) The Data Protection Laws (GDPR) to intensify the privacy & security cocktail: understanding the data protection rights offered by the GDPR to empower individuals to use and practice privacy (offered by Privacy Algebra); Q&A
17:45-17:50	Closing (Imge Ozcan, Rocco Bellanova, Kirsten Fiedler)		
19:00- ...	After-party: Quiz and drinks @ Smouss Bar		

09:30-10:00 COFFEE

10:00-10:15 WELCOME (Auditorium 3)

10.30 – 12.00 SESSIONS

10.30 – 12.00 Salle du Conseil, 4th floor
1. EDPS-Civil Society Summit 2018

Welcome and introduction:

- Wojciech Wiewiorowski, Assistant European Data Protection Supervisor

Moderator/co-chair:

- Sari Depreeuw, ProfessorProfessor at Université Saint Louis Bruxelles, Senior Researcher at LSTS (Vrije Universiteit Brussel), Partner at law firm DALDEWOLF

10.05-10.45 Session 1. Challenges to GDPR implementation: individual and collective redress

Input by:

- Katarzyna Szymielewicz, President of the Panoptykon Foundation, Vice-President EDRi
- Javier Ruiz Díaz, Policy Director at the Open Rights Group

Discussion

10.45-11.25 Session 2: Monitoring illegal content online: notice and action procedures

Input by:

- Maryant Fernández Pérez, Senior Policy Advisor at EDRi
- Fanny Hidvegi, European Policy Manager at Access Now

Discussion

Closing remarks:

- Giovanni Buttarelli, European Data Protection Supervisor

10.30 – 12.00 Auditorium 3
2. Digital Privacy – low and high hanging fruits, and how to pick them

The internet is broken and we need to do something about it! Hackers, techies and scientists are working on the different solutions – most of them just fighting the symptoms, instead of curing the roots: Many solutions to protect communication (like email, IM, chats) provide encryption – this protects the actual content of your communication, but the metadata still stays visible (who talks to whom, how much, how often, from which place, etc). Other solutions to protect information- and file sharing (mostly happening through the wold wide web) provide some protection against parties that track you, or obfuscate and hide your presence in the network. All of them work with the current state of the internet that has been designed in the 70-ies.

In this session, we will explain the underlying problems with the current state of the Internet and we want to show how to solve them on the long run: A next generation of decentralised Internet protocols to create a new Internet with end-to-end encryption and anonymisation of data flows. But since this solution will take a while to implement, we will also highlight short-term solutions: For instance, new ways to encrypt your interpersonal communication without much hassle for the user – and give an overview of the various options and ways to hide and obfuscate your presence in the world wide web.

The session will conclude with an interactive mapping exercise in terms of available free/libre and open source tools for people to defend themselves, focusing mostly on the browser extensions/mobile apps space, and look at the obvious gaps in capabilities that could be filled in the future.

Speakers:

- sva, pEp Foundation
- Nana Karlstetter, pEp Foundation
- Walter van Holst, Vrijschrift

12.00 – 13.00 LUNCH BREAK

13.00 – 14.30 SESSIONS

13.00 – 14.30 Auditorium 3
1. Round-table: Government hacking in different national contexts & strategies for challenging surveillance

An increasing number of governments are adopting hacking techniques to facilitate their surveillance activities. Hacking is a particularly novel surveillance technique that raises new challenges. We urgently need to come together as civil society actors from diverse jurisdictions to discuss strategies for challenging or curtailing this power.

This session will be designed as a roundtable moderated by Privacy International. It will be broken down into two 45-minute segments as follows:

(1) Hacking in Different National Contexts (45 min.)

The first 45-minute segment will feature short (max. 5 minute) presentations by different civil society organisations. These presentations will touch upon government hacking developments in their respective national contexts and any ongoing legal or advocacy work to address these powers.

(2) Strategies for Challenging State Hacking for Surveillance (45 min.)

The second 45-minute segment will be an open discussion moderated by Privacy International on strategies for challenging state hacking for surveillance. This discussion may include the following topics:

- What are strategies to unmask government hacking?
- What are strategies to challenge government hacking?
- What are strategies to limit government hacking?
- What are strategies for combating government efforts to compel companies to facilitate hacking?

Moderators:
- Tomaso Falchetta, Legal officer at Privacy International
- Scarlet Kim, Legal Officer at Privacy International

13.00 – 14.30 Auditorium 4
2. From "old" filter bubbles to political microtargeting

How powerful is the profiling on social media? How to increase its accountability?

Social media companies have undoubtedly a great impact on the shape of public discourse and how we access information. For the majority of internet users, social media is the gateway to learn about the news, get a sense of what other think and to share their own opinions.

At the same time those companies are not taking civic responsibilities even though their algorithms are central to how information is consumed in the world today. The business model of social media platforms such as Facebook and Twitter is based on monetising user traffic which enable clickbait and misinformation to proliferate.

While filter bubbles are not unique to social networks, we are still far from understanding their mechanics and potential effects on the society. Similar concerns relate to the use of microtargeting in social media...

Is election politics being re-shaped in the digital age? Should we expect more transparency and accountability from social media companies with regard to algorithms and targeting techniques they use and how those tools are used in political campaigns? Can data protection law help us in this fight?

Speakers:

- Katarzyna Szymielewicz, Panoptykon Foundation (PL)
- Jeffrey Chester, Center for Digital Democracy (USA)
- Frederike Kaltheuner, Privacy International (UK)

Moderator:

- Rocco Bellanova, University of Amsterdam and Université Saint-Louis - Bruxelles

14.30 – 14.45 COFFEE BREAK

14.45 – 16.00 SESSIONS

14.45 – 16.00 Auditorium 3
1. Exchange with policy-makers: Government hacking for surveillance

This session will bring European and national policy-makers and experts to discuss emerging efforts to regulate government hacking as a form of surveillance.

Presentations on some of the key challenges surrounding government hacking will be followed by a Q&A.

Among the questions to be addressed:

- Why do governments hack?
- How do we conceptualise cybersecurity? What are the challenges in defending cybersecurity? How do we embed cybersecurity into discussions about government hacking?
- What are the challenges in regulating government hacking?
- Are some methods of acquiring vulnerabilities and exploits off-limits or should they be? Which ones?
- Should governments ever use zero-days to hack? Should they be limited to using known vulnerabilities? Should they be permitted to impersonate known and trusted third parties?
- What should the relationship be between vulnerability disclosure and government hacking?
- What recourse should there be for those who have been collaterally affected?

Speakers:

- Ralf Bendrath, Senior Policy Adviser, European Parliament
- Juraj Sajfert, Policy Officer, European Commission, DG Justice and consumers
- Kees Verhoeven, Dutch MP, Democrats 66 [TBC]
- Raphaël Vinot CERT Operator, CIRCL – Computer Incident Response Center Luxembourg

Moderator:

- Scarlet Kim, Legal Officer, Privacy International

14.45 – 16.00 Auditorium 4
2. Investigating algorithmic systems: Algorithm auditing

Algorithms are playing a crucial role in all aspects of life from employment decisions, to credit scores to criminal justice processes. They are being used to make very important decisions which have life-changing consequences and these decision-making processes are largely unaudited. An algorithm is a procedure or a formula often used by a computer to solve a problem. Many algorithms are proprietary and secret which hinder investigating them. However, there is a pressing need to study algorithms empirically, especially to test their fairness. This panel will discuss algorithm auditing as a research design and regulatory tool to identify bias and increase algorithmic accountability.

Speakers:

- Marc Rotenberg, EPIC
- Bettina Berendt, Department of Computer Science, KU Leuven
- Juhi Kulshrestha, Hans Bredow Institute for Media Research at Hamburg University
- Michael Veale, UCL STEaPP

Moderator:

- Joris van Hoboken, VUB-LSTS

16.00 – 16.15 COFFEE BREAK

16.15 – 17.45 SESSIONS

16.15 – 17.45 Auditorium 3
1. The use of AI by public authorities

Automated systems are increasingly part of our everyday lives – from scanning faces in airports and train stations, to shopping recommendations, to using facebook posts for insurance purposes. These systems are usually based on massive data collections and profiling which raise concerns that go well beyond the protection of personal data and privacy.

A number of public authorities are already partnering up with companies to develop AI and discuss its use, leading to challenging questions for civil and human rights as well as democracy. For example, in the US, the police's body cams footage is used to train machine vision algorithms for law enforcement. Germany recently started testing new voice recognition software that can tell which country migrants without documentation come from. Similar use of algorithms or automated systems are also in use in Italy, France, the UK, China, India and soon probably at all EU borders.

Faced with the raise of populist and euro-sceptic movements across Europe, what does the increase use of AI by public authorities mean for human rights?

The goal of this session is to launch a process for the drafting of civil society recommendations for public authorities' use of machine learning/AI and other automated decision making systems. Ideally, based on the outcomes of the panel, a first draft could be developed between January to May to be presented at RightsCon 2018.

Speakers:
- Varoon Bashyakarla, Tactical Tech
- Frederike Kaltheuner, Privacy International
- Estelle Masse, Access Now
- Jay Stanley, ACLU

Moderator:
- Maryant Fernández Pérez, Senior Policy Advisor at EDRi

Privacy Camp 2018

SPEECH, SETTINGS AND [IN]SECURITY BY DESIGN

23 January 2018 | Brussels, Belgium | #PrivacyCamp18

16.15 – 17.45 Auditorium 3
2. Strip searching the internet

Fuelled by war on terrorism, the fake news debate and the fight against infringing content, there is an increasing stream of legislative proposals across Europe and the globe that invade online privacy and limit digital free speech in the name of law enforcement.

The currently discussed EU Copyright Directive includes a requirement for major online services to install upload filters that monitors everything for possible copyright infringement in order to avoid liability. In the UK content take-downs with the aim of hindering the spreading of terrorist content are becoming the norm. Across the continent hate speech and fake news are leading or have led to content blocking & removal legislation.
But are these measure effective and what are their effects? And is the urge to control content and take it down instantly not leading to blanket surveillance of all online activity?

Speakers:

- Glyn Moody, Writer, journalist, blogger
- Anni Hellmann, Unit I4, DG CNECT at the European Commission
- Slavka Bielikova, Open Rights Group
- Melody Patry, Access Now

Moderator:

- Dimitar Dimitrov, EU Policy Director at Wikimedia

17.45 – 18.00 CLOSING

19.00 onwards
AFTER-PARTY
@ Smouss Café

- with a quiz &
free drinks for those
bringing their
conference badge!

ORGANISED BY

EDRi

PRIVACY SALON

www.privacysalon.org

UNIVERSITÉ SAINT-LOUIS BRUXELLES

LSTS LAW, SCIENCE, TECHNOLOGY & SOCIETY STUDIES VRIJE UNIVERSITEIT BRUSSEL

iee Institut d'études européennes Institute for European Studies

11th INTERNATIONAL CONFERENCE
24 25 26 JANUARY 2018 BRUSSELS, BELGIUM
COMPUTERS, PRIVACY & DATA PROTECTION
CPDP2018
THE INTERNET OF BODIES
WWW.CPDPCONFERENCES.ORG

SUPPORTED BY:

moz://a

TOMTOM

STAY IN TOUCH! #PrivacyCamp2018

https://twitter.com/edri
https://twitter.com/CPDPconferences
email: brussels@edri.org

The conference presentations will be made available online: https://privacycamp.eu/

DONATE TO EDRi
https://edri.org/donate/