Report from Dagstuhl Seminar 25042

Online Privacy: Transparency, Advertising, and Dark Patterns

Günes Acar*[1], Nataliia Bielova*[2], Zubair Shafiq*[3], and Frederik Zuiderveen Borgesius*[4]

1 **Radboud University Nijmegen, NL.** g.acar@cs.ru.nl
2 **Inria centre at University Côte d'Azur – Sophia Antipolis, FR.** nataliia.bielova@inria.fr
3 **University of California – Davis, US.** zubair@ucdavis.edu
4 **Radboud University Nijmegen, NL.** frederik.zuiderveenborgesius@ru.nl

Abstract

This report documents the program and the outcomes of Dagstuhl Seminar 25042 "Online Privacy: Transparency, Advertising, and Dark Patterns". The seminar brought 26 participants in computer science, law and policy together, coming from research institutions, as well as industry, law firms and regulators across Europe, US, and Middle East.

The 2.5-day seminar had a well-filled program, with introductions of all participants and several group activities; two presentations from industry representing Web browser providers, such as Apple and Mozilla; two presentations from the law research community presenting open problems in Web tracking, dark patterns, ad tech and new EU regulations, such as the EU Digital Services Act; and two panels – one presenting the open challenges in compliance by EU and US lawyers and regulators, and one discussing the future of advertising by industrial representatives from Web browser vendors. The program also included a rump session for short talks, allowing all participants to expose their recent research, open questions, and challenges to these research communities, industry, and regulators.

Seminar January 19–22, 2025 – https://www.dagstuhl.de/25042

2012 ACM Subject Classification Security and privacy → Browser security; Security and privacy → Human and societal aspects of security and privacy; Security and privacy → Privacy-preserving protocols; Security and privacy → Pseudonymity, anonymity and untraceability; Security and privacy → Social network security and privacy; Security and privacy → Web application security; Networks → Web protocol security; Information systems → World Wide Web

Keywords and phrases advertising, dark patterns, data protection, online tracking, privacy, world wide web

Digital Object Identifier 10.4230/DagRep.15.1.122

* Editor / Organizer

Online Privacy: Transparency, Advertising, and Dark Patterns, *Dagstuhl Reports*, Vol. 15, Issue 1, pp. 122–135
Editors: Günes Acar, Nataliia Bielova, Zubair Shafiq, and Frederik Zuiderveen Borgesius

Dagstuhl Reports
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

1 Executive Summary

Günes Acar (Radboud University Nijmegen, NL)
Nataliia Bielova (Inria centre at University Côte d'Azur – Sophia Antipolis, FR)
Zubair Shafiq (University of California – Davis, US)
Frederik Zuiderveen Borgesius (Radboud University Nijmegen, NL)

The Dagstuhl Seminar on *Online Privacy: Transparency, Advertising, and Dark Patterns* enhanced the collective understanding of changes in online tracking, advertising, and dark patterns within an interdisciplinary research community in computer science and law. Following the success of the 2017 Dagstuhl Seminar "Online Privacy and Web Transparency", this seminar brought together experts from academia, legal professionals, regulators, and industry to tackle novel challenges emerging from the shifting technological and regulatory landscape.

More than half a decade after the 2017 seminar, some of the familiar questions have resurfaced in new contexts, such as smart devices and augmented reality. The introduction of privacy regulations and enforcement regimes around the world has prompted and enabled a slew of new research. Meanwhile, browsers and mobile platforms have started shipping built-in anti-tracking features, and a once-in-a-generation redesign of the online advertising and tracking ecosystem is underway.

Spanning three days, the seminar featured a variety of session formats including short talks, interactive demos, and moderated brainstorming sessions. Bringing together researchers and industry experts, the seminar promoted collaboration and advanced research on these challenges, while also exploring future research directions. Topics that were discussed during the seminar included the following:

Online Tracking Beyond Cookies

- How should online tracking research respond to fundamental changes in tracking mechanisms after the third-party cookie phaseout?
- Which techniques, tools, and methods could prove beneficial and are currently absent in researchers' toolboxes?
- Do existing regulations provide sufficient protection against novel types of tracking and profiling?
- How can computer science research help regulators with enforcement of regulations, or with developing better regulations?

Alternative Advertising Mechanisms

- What are the potential abuses associated with the novel advertising mechanisms (e.g., Topics API, Protected Audience API), and what measures can be implemented to monitor and prevent them?

Dark Patterns and Online Manipulation

- What methods and strategies are effective for detecting privacy-related dark patterns in various contexts, and how do these dark patterns influence both immediate and future privacy decisions of users?

Structure of the 3-day seminar

Day 1 – morning A plenary opening session laying the ground for the seminar, presentation of the main research topics and statistics on the participants topic interest, field of work, and background, was given to quickly foster exchanges since computer science and law experts often express the will to exchange but do not have the opportunity. Therefore, the seminar started with two sessions that enabled everybody to introduce themselves to the others. The morning session was followed by informal voting on the participants' interests in the proposed main topics and background. Topics for further discussion in working groups were identified.

Day 1 – afternoon The first session consisted of group activities on identified topics and a report of the main outcomes in the plenary session. The afternoon continued with the presentation of a browser vendor representative presenting the open problems in web tracking from an industry perspective. The last session in the afternoon featured a panel with lawyers and regulators discussing open problems in compliance, regulation, and enforcement from the EU and US perspectives.

Day 2 – morning The first session of presentations from an academic researcher on privacy signals and a browser vendor were appreciated by the participants. The morning session was followed by further group activities to discuss new topics of interest that evolved since Day 1. The morning finished with a wrapping-up session presenting the results of each group discussion.

Day 2 – afternoon The afternoon contained two sessions: presentations from legal scholars on the challenges and advancements in the EU law and new forms of transdisciplinary research between computer science and law researchers. The second session offered a panel with browser vendors, presenting unique insights into their challenges with online tracking, regulation and dark patterns to the audience.

Day 3 – morning On Day 3, there was a session with short (5 minutes) rump session talks. There was also a collective discussion on the main takeaways of the seminar with collection of feedback from the participants. It was followed by an informal session to foster further exchanges between participants who have identified common topics of interest.

Results, summary

- The seminar enhanced the collective understanding of changes in online tracking, advertising and dark patterns within an interdisciplinary research community in computer science and law.
- The seminar built a community of researchers from different disciplines who are interested in online privacy, and established further exchanges with industry and regulators.
- The seminar fostered transdisciplinary cooperation for research and future grant proposals, such as EU grants (EU collaborative projects and ERC synergy grant), bilateral agreement grants within EU countries but also EU-US, and EU-India.
- The seminar raised awareness among participating researchers about the challenges and opportunities for collaboration across computer science and law disciplines, leading to better understanding of empirical research.
- During the seminar, several participants formed interdisciplinary teams to collaborate on papers and grant proposals in the future. One of the already visible outcomes of the seminar is a new article co-authored by several participants surveying the advances and open problems in web tracking [1].

- A collaboration that started at our seminar led to the discovery of a previously undocumented tracking method, used by Meta and Yandex to track billions of Android users. The investigation led by two attendees of our seminar resulted in defenses deployed by browser vendors including Chrome and Firefox, and termination of the tracking campaign by the companies [2].

References

1 SoK: Advances and Open Problems in Web Tracking. Y. Vekaria, Y. Beugin, S. Munir, G. Acar, N. Bielova, S. Englehardt, U. Iqbal, A. Kapravelos, P. Laperdrix, N. Nikiforakis, J. Polakis,F. Roesner, Z. Shafiq, S. Zimmeck. Online report, June 2025. https://arxiv.org/abs/2506.14057

2 Covert Web-to-App Tracking via Localhost on Android. Aniketh Girish, Günes Acar, Narseo Vallina-Rodriguez, Nipuna Weerasekara, Tim Vlummens. Online report, June 2025. https://localmess.github.io

2 Table of Contents

3 Overview of Talks

3.1 Dark Patterns as Legal Violations in Web Tracking

Cristiana Santos (Utrecht University, NL)

Joint work of Cristiana Santos, Nataliia Bielova, Colin Gray, Johana Gunawan, Sanju Ahuja, Christine Utz
Main reference Colin M. Gray, Cristiana Teixeira Santos, Nataliia Bielova, Thomas Mildner: "An Ontology of Dark Patterns Knowledge: Foundations, Definitions, and a Pathway for Shared Knowledge-Building", in Proc. of the CHI Conference on Human Factors in Computing Systems, CHI 2024, Honolulu, HI, USA, May 11-16, 2024, pp. 289:1–289:22, ACM, 2024.
URL https://doi.org/10.1145/3613904.3642436

Extant regulations worldwide govern dark patterns explicitly or implicitly. EU member states and US states' own statutes and enforcers, as well as other union-wide legislation or authorities may also regulate some types of dark patterns or related behaviours – or otherwise issue guidance. A growing body of enforcement actions and regulatory fines globally currently comprise a strong approach for dark patterns general deterrence [1]. In this talk, I discuss web tracking practices that may constitute legal violations under the GDPR, ePD, and can be aligned with dark patterns. Aligning non-compliant online tracking practices with dark pattern prohibitions enhances dark pattern general deterrence. I report several instances thereof based on our legal-empirical research.

- Publishers and CMPs don't respect users' choice [2, 3]:
  - consent banner stores a positive consent even when the user refused consent, corresponding to the dark pattern of sneaking;
  - a positive consent is stored before the user made a choice, corresponding to the dark pattern of sneaking;
  - the consent request does not offer a way to refuse consent, corresponding to the dark pattern of obstruction;
  - Some purposes or advertisers are pre-selected: pre-ticked boxes or sliders set to "accept", corresponding to the dark pattern of bad defaults.
- CMP website scanners are used as compliance solutions, though these introduce:
  - false negatives: only scans cookies, but miss other tracking technologies, such as browser fingerprinting, and as such, data is processed without legal basis [4], which corresponds to the dark pattern of 'hidden information';
  - false positives: scanners deceive editors that a consent banner is needed on an empty website without any trackers [5], aligned with the dark pattern of 'forced action'.
- The QuantCast CMP banner sets and sends QuantCast cookie to its server without a legal basis, potentially infringing the lawfulness and fairness principles, and this practice can qualify the dark pattern of sneaking and forced action [4].
- Pay or ok models offer 2 options to end-users in order to gain access to an online service: i) consent to being tracked and targeted with behavioural advertising, or ii) pay a ad-tracking fee. Dark Patterns also occur in the "Pay or Ok models" [6] where social engineering dark patterns appear under the pay option.
- Google Tag Manager (GTM) facilitates inclusion of third-party JS and is used on 62% on top of 100k websites. Within the GTM ecosystem, 780 not-supported Google tags are hidden, Google-owned tags are instead featured on top, and 67 tags supported by Google are only shown at the bottom, which configure the dark patterns of false-hierarchy and Adding Steps [7].

References

1 An Ontology of Dark Patterns Knowledge: Foundations, Definitions, and a Pathway for Shared Knowledge-Building, 2024. Colin M. Gray, Cristiana Santos, Nataliia Bielova, and Thomas Mildner. In Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems (CHI '24).
2 Do Cookie Banners Respect my Choice? Measuring Legal Compliance of Banners from IAB Europe's Transparency and Consent Framework, 2020. Célestin Matte, Nataliia Bielova, Cristiana Santos. IEEE Symposium on Security and Privacy, 2020.
3 Dark Patterns and the Legal Requirements of Consent Banners: An Interaction Criticism Perspective, 2021. Colin M. Gray, Cristiana Santos, Nataliia Bielova, Michael Toth, Damian Clifford. ACM CHI Conference on Human Factors in Computing Systems (CHI '21).
4 Consent Management Platforms under the GDPR: processors and/or controllers? 2021. Cristiana Santos, Midas Nouwens, Michael Toth, Nataliia Bielova, Vincent Roca. In Privacy Technologies and Policy: 9th Annual Privacy Forum.
5 On dark patterns and manipulation of website publishers by CMPs. Michael Toth, Nataliia Bielova, Vincent Roca. Privacy Enhancing Technologies Symposium, 2022.
6 Legitimate Interest is the New Consent – Large-Scale Measurement and Legal Compliance of IAB Europe TCF Paywalls. Victor Morel, Cristiana Santos, Viktor Fredholm, and Adam Thunberg. 2023. In Proceedings of the 22nd Workshop on Privacy in the Electronic Society (WPES '23).
7 Which Online Platforms and Dark Patterns Should Be Regulated under Article 25 of the DSA? 2024, Cristiana Santos, Nataliia Bielova, Sanju Ahuja, Christine. Utz, Colin Gray, Gilles Mertens, Preprint: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4899559

3.2 Studying Privacy Threats in Complex and Interconnected Platforms: The Case of Smart Homes

Narseo Vallina-Rodriguez (IMDEA Networks Institute – Madrid, ES)

Joint work of Aniketh Girish, Tianrui Hu, Vijay Prakash, Daniel J. Dubois, Srdjan Matic, Danny Yuxing Huang, Serge Egelman, Joel Reardon, Juan Tapiador, David R. Choffnes, Narseo Vallina-Rodriguez
Main reference Aniketh Girish, Tianrui Hu, Vijay Prakash, Daniel J. Dubois, Srdjan Matic, Danny Yuxing Huang, Serge Egelman, Joel Reardon, Juan Tapiador, David R. Choffnes, Narseo Vallina-Rodriguez: "In the Room Where It Happens: Characterizing Local Communication and Threats in Smart Homes", in Proc. of the 2023 ACM on Internet Measurement Conference, IMC 2023, Montreal, QC, Canada, October 24-26, 2023, pp. 437–456, ACM, 2023.
URL https://doi.org/10.1145/3618257.3624830

Privacy risks may occur when platforms, software, and devices interact with other colluding elements in the local network using wireless interfaces like WiFi or Bluetooth[1]. However, the research community has typically followed a process-centric and monolithic approach to detect such abuses in modern consumer-oriented software, while current privacy controls are not fit to limit side-channels and covert-channels that exist in such interconnected environments.

The network communication between Internet of Things (IoT) devices on the same local network has significant implications for platform and device interoperability, security, privacy, and correctness. Yet, the privacy issues of local home Wi-Fi network traffic and its associated security and privacy threats have been largely ignored by prior literature. In this talk, I presented the results of a comprehensive and empirical measurement of the interactions that occur between devices on the local network and its threats [2]. Our analysis reveals vulnerable devices, insecure use of network protocols, and sensitive data exposure by IoT

devices. We provide evidence of how this information is exfiltrated to remote servers by mobile apps and third-party SDKs, potentially for household fingerprinting, surveillance, and cross-device tracking.

References

1 A. Girish, J. Reardon, S. Matic, J. Tapiador, and N. Vallina-Rodriguez. Your Signal, Their Data: An Empirical Privacy Analysis of Wireless-scanning SDKs in Android. PETS Symposium 2025 (To Appear)
2 A. Girish, T. Hu, V. Prakash, D. Dubois, S. Matic, D. Huang, S. Egelman, J. Reardon, J. Tapiador, D. Choffnes, and N. Vallina-Rodriguez. In the Room Where It Happens: Characterizing Local Communication and Threats in Smart Homes. ACM IMC 2023.

3.3 Global Privacy Control in EU Data Protection Laws

Sebastian Zimmeck (Wesleyan University – Middletown, US)

Joint work of Katherine Hausladen, Oliver Wang, Sophie Eng, Jocelyn Wang, Francisca Wijaya, Matthew May, Sebastian Zimmeck
Main reference Katherine Hausladen, Oliver Wang, Sophie Eng, Jocelyn Wang, Francisca Wijaya, Matthew May, Sebastian Zimmeck: "Websites' Global Privacy Control Compliance at Scale and over Time" 34th USENIX Security Symposium (USENIX Security) Seattle, CA, August 2025
URL https://sebastianzimmeck.de/hausladenEtAlGPCWeb2025.pdf

The California Consumer Privacy Act (CCPA) gives California residents the right to opt out of the sale or sharing of their personal information via Global Privacy Control (GPC). Similar other states in the US also give their residents a right to opt out via GPC. However, how can GPC be applied in the European Union? GPC is adaptable to various laws as it is does not prescribe a particular meaning to what a GPC signal means beyond the general meaning of opting out. Thus, it is the task of legislators and regulators in every jurisdiction to fill GPC with life. This talk highlighted how GPC works, its adoption in the US, and how it could work in the EU. To map GPC to the GDPR the legal basis for processing can be taken into account: (1) where the legal basis is consent, the data subject is withdrawing their consent under Article 7(3) specifically to processing by data controllers other than the first party and to processing of the first party to transfer data to other data controllers, (2) where the legal basis is legitimate interest or public interest, the data subject is objecting to processing by data controllers other than the first party and to processing of the first party to transfer data to other data controllers under Article 21(1-3, 5), and (3) where the legal basis is contractual, legal obligation, or vital interests the signal has no effect [1].

References

1 Berjon Robin. *GPC under the GDPR*. https://berjon.com/gpc-under-the-gdpr/, 2021

3.4 The EU Digital Services Act: what does it mean for online advertising and adtech?

Frederik Zuiderveen Borgesius (Radboud University Nijmegen, NL)

What does the Digital Services Act (DSA) mean for online advertising? We describe and analyse the DSA rules that are most relevant for online advertising and adtech (advertising technology). We also highlight to what extent the DSA's advertising rules add something to the rules in the General Data Protection Regulation (GDPR) and the ePrivacy Directive. The DSA introduces several specific requirements for online advertising. First, the DSA imposes transparency requirements in relation to advertisements. Second, very large online platforms (VLOPs) should develop a publicly available repository with information about the ads they presented. Third, the DSA bans profiling-based advertising (behavioural advertising) if it uses sensitive data or if it targets children.

Besides these specific provisions, the general rules of the DSA on illegal content also apply to advertising. Advertisements are a form of information, and thus subject to the general DSA rules. Moreover, we conclude that the DSA applies to some types of ad tech companies. For example, ad networks, companies that connect advertisers to publishers of apps and websites, should be considered platforms. Some ad networks may even qualify as VLOPs.

Hence, ad networks must comply with the more general obligations in the DSA. The application of these general rules to advertisements and ad networks can have far-reaching effects that have been underexplored and deserve further research. We also show that certain aspects of the DSA are still unclear. For instance, we encourage the European Commission or regulators to clarify the concepts of 'online platform' and 'recipients' in the context of ad networks and other adtech companies.

4 Panel discussions

4.1 Panel: collective discussions on main takeaways of the seminar

Günes Acar (Radboud University Nijmegen, NL), Nataliia Bielova (Inria centre at University Côte d'Azur – Sophia Antipolis, FR), Zubair Shafiq (University of California – Davis, US), and Frederik Zuiderveen Borgesius (Radboud University Nijmegen, NL)

Browser Ecosystem and Collaboration

Browsers have undergone significant evolution over time, and this progress underscores the fact that laws – and the ways in which they are interpreted – also continuously change. Engaging with actors outside of academia, such as reporters, is important for effectively disseminating research findings to broader audiences. The browser vendor panel proved to be particularly valuable, as it revealed relationships among vendors that were previously unknown. This highlights the importance of fostering collaboration and dialogue between the research community and the browser ecosystem.

Security and Standardization

There is much to be learned from the security community, particularly in how it clearly defines and responds to various behaviors. It is important to clarify which behaviors are considered good, bad, or deceptive, and to establish mechanisms to block, prevent, or mitigate the harmful ones. A key challenge lies in identifying an appropriate venue for standardizing these efforts, with peer-reviewed journals suggested as a possible avenue.

Privacy, Manipulation, and Public Concerns

Concerns have been raised about the increasing reliance on tools like ChatGPT, particularly regarding the potential for manipulation and the implications for monopolistic control. This situation emphasizes the importance of being able to articulate privacy risks with clarity, both for public understanding and for informing policy and technical responses.

Research Directions in Privacy

There is a need for further research aimed at exposing and explaining privacy risks in digital environments. One important area of study involves demonstrating how tracking can be unavoidable under current conditions. This seminar was especially convincing in showing that the study of dark patterns can be approached as a scientific discipline, worthy of systematic investigation.

Mitigation Strategies and Standards

Conducting breakage analysis could be a valuable tool in the design of effective tracking mitigation strategies. Additionally, there may be a need to develop a framework similar to the "Better Ads Standard" to guide acceptable tracking practices and support a more privacy-respecting web ecosystem.

Privacy Signals

Privacy standards are challenging to develop because individuals and organizations operate with different threat models. The talk on privacy signals, such as Global Privacy Control (GPC), was found to be particularly interesting. It raised important questions about what changes might be needed from browser vendors to better support such signals. Topics discussed included the role of dark patterns in consent dialogs, the ongoing risk posed by fingerprinting techniques, and the possibility of a class action emerging in Europe related to these privacy concerns.

Impact on regulatory compliance

Participants discussed the limitations of regulators, particularly their geographical constraints, and debated whether naming and shaming actually leads to reform or merely pushes dark patterns elsewhere. It was noted that vague warnings like "thousands of websites tracking you" are ineffective; instead, there is a need to clearly articulate specific harms and improve communication strategies. The group considered major challenges in the field, balancing pessimism with activism, and noting that even large fines, like Meta's 13 billion USD, might indicate that regulation can have some impact. There was optimism in seeing regulators' receptiveness and recognition that most users cannot be expected to understand how the underlying technology works.

Future challenges

The seminar sparked many new research directions and provided valuable insights, including developer perspectives. One attendee called it "probably the best Dagstuhl I've been to." There was reflection on whether the privacy battle has already been lost due to the vast trails of data left behind, raising the question of whether current efforts are more for the benefit of future generations. Collaborative work with browser vendors was highlighted as a path to meaningful change. Cross-disciplinary exchange – especially with legal experts – was seen as a major strength of the seminar, though it was also noted that economists were absent from the discussion. Finally, ethical questions about the strategy of naming and shaming were raised, signaling a need for deeper consideration of advocacy tactics.

4.2 Panel: Compliance, Regulation and Enforcement

Günes Acar (Radboud University Nijmegen, NL), Nataliia Bielova (Inria centre at University Côte d'Azur – Sophia Antipolis, FR), Zubair Shafiq (University of California – Davis, US), and Frederik Zuiderveen Borgesius (Radboud University Nijmegen, NL)

The panel took place at the end of Day 1 and the panelists were: Jason "Jay" Barnes (Simmons Hanly Conroy); Lesley E. Weaver (Bleichmar Fonti & Auld); Vincent Toubiana (CNIL); Frederik Zuiderveen Borgesius (moderator):

Jason "Jay" Barnes Attorney Jason "Jay" Barnes is a partner at Simmons Hanly Conroy in the Complex Litigation Department where he focuses his practice on consumer class action lawsuits. Before joining the firm, Jay served eight years as a state representative in the Missouri General Assembly. In this role, he fought against fraud, abuse and waste as chairman of the House Committee on Government Oversight and Accountability. He also served as chairman of the Special Investigative Committee on Oversight formed in 2018 to investigate the wrongdoings of former Missouri governor Eric Greitens. https://www.simmonsfirm.com/about-us/our-attorneys/jason-barnes/

Lesley E. Weaver Lesley joined Bleichmar Fonti & Auld LLP as a partner in 2016, opening the firm's California office. In her twenty year career, Lesley has focused primarily on cases that protect the public interest, consumers, and public entities. As part of her mission to protect the public trust, Lesley also serves as counsel to a number of governmental entities, in both formal and informal roles. Lesley represents the Cities of Palo Alto and Richmond, California in a municipal subclass in In re Lithium Ion Batteries Antitrust Litig. Lesley also represents Oakland County, Michigan in In re Liquid Aluminum Sulfate Antitrust Litig. Lesley is committed to public service through volunteer efforts, and currently serves on the Advisory Council of the East Bay Community Law Center, as well as the Executive Committee of the Securities Section for the Bar Association of San Francisco. https://www.bfalaw.com/professionals/lesley-weaver

Vincent Toubiana Vincent works at the CNIL, the Commission Nationale de l'Informatique et des Libertés. The CNIL is the French Data Protection Authority. Vincent has been head of CNIL's digital innovation lab (the LINC) since 2021. He obtained a PhD "Computer Science and Networks" from Telecom ParisTech in 2008. He has worked on privacy since 2009. First at NYU under the direction of Helen Nissenbaum, then from 2010 to 2013, at Alcatel-Lucent Bell-Labs. He joined CNIL in 2013 as a technologist. In 2016, he was an International fellow at the Federal Trade Commission.

Frederik Zuiderveen Borgesius Frederik is professor of ICT and law. He works at the iHub, part of Radboud University in The Netherlands. The iHub is the interdisciplinary research hub on digitalization and society. Frederik is a law professor but teaches mostly at the computer science department. His research predominantly concerns fundamental rights, such as the right to privacy and non-discrimination rights, in the context of new technologies. He often enriches legal research with insights from other disciplines. He has cooperated with, for instance, economists, computer scientists, and communication scholars. He regularly advises policymakers, and has given expert testimony at the Dutch and the European parliaments, and committees of the Council of Europe and the United Nations. `https://www.ru.nl/personen/zuiderveen-borgesius-f/`

Overview of the discussion

The panel focused on the discussion of law and legal compliance, in particular relevant law in the US and the EU. The discussed topics included lessons learned from the 5+ years of GDPR; obstacles to enforcement and litigation in the EU and US; experiences from the US case law; insights on improving the exchanges and relations between regulators and researchers; recent new regulations in the EU and the United States, such as the EU Digital Service Act (DSA), the California Privacy Rights Act (CPRA) and decisions by the US Federal Trade Commission (FTC).

Differences in the EU and US laws related to privacy

During the panel there was quite some discussion about the differences between the law in the EU and the US. For instance, in the US, (private law) court cases between groups of claimants against companies play a large role in privacy law. In the EU, such cases are rare. Meanwhile, in the EU, there are many cases in which Data Protection Authorities enforce the GDPR. Such enforcement actions sometimes lead to (administrative law) court cases between the Data Protection Authority and the company.

Exposing research results to regulators

All participants expressed interest in new empirical findings about online tracking by academic researchers. Yet, lawyers and regulators rarely have time to read through the full academic publications, pointing out that blog posts about academic findings would be more appreciated. Additionally, similarly to the FTC's PrivacyCon in-house conference, the CNIL organizes a yearly event, called Privacy Research Day, where researchers are invited to submit their contributions to achieve a higher visibility and impact of their research results.

4.3 Panel: Browser vendors: Future of tracking and advertising

Nataliia Bielova (Inria centre at University Côte d'Azur – Sophia Antipolis, FR), Günes Acar (Radboud University Nijmegen, NL), Zubair Shafiq (University of California – Davis, US), and Frederik Zuiderveen Borgesius (Radboud University Nijmegen, NL)

The panel took place at the second day of the seminar and the panelists were as follows: Igor Bilogrevic (Google); Hamed Haddadi (Imperial College London/Brave); Anastasia Shuba (DuckDuckGo); John Wilander (Apple); Martin Thomson (Mozilla), moderator.

With participants from five different browser vendors, the panel focused on the future of tracking and advertising, in light of recent regulatory changes, efforts such as Privacy Sandbox and rise of LLMs.

Participants highlighted breakage (e.g. bug due to tracking mitigations) being a significant challenge for shipping tracking defenses. It was noted that vendors could better communicate both among themselves and with wider research community.

The impact of AI taking over web search was discussed, with questions raised about the sustainability of the web in such a future. Concerns about the future of tracking (e.g. in LLM-based chat interfaces) and privacy problems that might arise ten years from now were also discussed in hypothetical terms.

Overall, the panel provided rare insights into challenges faced by the browser vendors who aim to develop and ship more tracking defenses. In the post-seminar survey, several participants indicated this panel to be one of their favorite throughout the seminar.

Participants

- Günes Acar
Radboud University
Nijmegen, NL
- Jason "Jay" Barnes
Simmons Hanly Conroy –
New York, US
- Nataliia Bielova
Inria centre at University Côte
d'Azur – Sophia Antipolis, FR
- Igor Bilogrevic
Google – Zürich, CH
- Yana Dimova
DistriNet, KU Leuven, BE
- Serge Egelman
ICSI – Berkeley, US
- Imane Fouad
INRIA Lille, FR
- Colin M. Gray
Indiana University –
Bloomington, US
- Johanna Gunawan
Maastricht University, NL
- Hamed Haddadi
Imperial College London, GB
- Martin Johns
TU Braunschweig, DE
- Konrad Kollnig
Maastricht University, NL
- Athina Markopoulou
University of California –
Irvine, US
- Rishab Nithyanand
University of Iowa –
Iowa City, US
- Cristiana Santos
Utrecht University, NL
- Zubair Shafiq
University of California –
Davis, US
- Anastasia Shuba
DuckDuckGo – Paoli, US
- Sandra Siby
New York University –
Abu Dhabi, AE
- Martin Thomson
Mozilla – Mountain View, US
- Vincent Toubiana
CNIL – Paris, FR
- Christine Utz
Radboud University
Nijmegen, NL
- Narseo Vallina-Rodriguez
IMDEA Networks Institute –
Madrid, ES
- Lesley E. Weaver
Bleichmar Fonti & Auld –
Oakland, US
- John Wilander
Apple – Cupertino, US
- Sebastian Zimmeck
Wesleyan University –
Middletown, US
- Frederik Zuiderveen Borgesius
Radboud University
Nijmegen, NL