Workshop on Empirical Privacy Studies
December 14, 2023

Time	Presentation	Location
09:00-11:00	PhD defense by Karel Kubicek	HG D 16.12
11:30-12:30	CLE Project Talks: Jakob Merane and Luca Baltensperger	CLA J 1
12:30-13:30	Finger Buffet Lunch	
13:30-14:15	Presentation by Nataliia Bielova (Inria Sophia Antipolis) & Cristiana Santos (Utrecht)	
14:15-15:00	Presentation by Amit Zac & Stefan Bechtold	
15:00-15:30	Coffee Break	
15:30-16:15	Presentation by Verena Zimmermann & Lorin Schöni	
16:15-17:00	Open Session moderated by Amit Zac	

09:00-11:00   **Kubicek Karel, Automated Analysis and Enforcement of Consent Compliance**

This dissertation explores the adherence of widespread data collection practices to privacy regulations, specifically focusing on cookies and emails governed by the ePrivacy Directive and GDPR. We employ machine learning and crawling methods to automate the detection of violations in both domains. Our analysis reveals an alarming prevalence of non-compliance in cookie notices (95%) and significant rates of invalid consents to marketing emails (22%). We propose to address these issues by automated enforcement. For instance, our browser extension CookieBlock utilizes machine learning for deleting unwanted cookies on the client side, efficiently enforcing the user consent and addressing the observed violations.

11:30-12:30   **CLE Project Talks**

Jakob Merane, The Deterrent Effect of Private GDPR Enforcement: First Evidence from the Google Fonts Dispute

Abstract: The enforcement of EU data privacy law is attracting growing attention. While academic research has mainly focused on public enforcement mechanisms, the General Data Protection Regulation (GDPR) also foresees private enforcement. Individuals can seek compensation for material or non-material damage in civil courts. Yet, no prior empirical study has explored the deterrent effect of this civil liability provision. This study offers initial insights into the effects of private legal actions in deterring non-compliance observed during the Google Fonts Dispute. Using panel data collected from the HTTP Archive, we implement a difference-in-difference approach. Our analysis reveals a significant reduction of a specific GDPR violation in countries affected by related private legal disputes. This decline is particularly pronounced after pre-lawsuit warning letter campaigns, as compared to the initial

court ruling. We argue that companies embraced a "wait and see" strategy following the ruling, but reacted strongly to the large-scale pre-lawsuits. We further investigate the role of company characteristics on compliance. Our results show that popular and larger companies, with a higher employee count, tend to adopt a more cautious approach compared to smaller, less popular companies. We argue that these differences are not driven by malicious intent but rather arise from factors such as increased modular reliance, limited legal and technical resources, and a lack of privacy awareness among small web developers.

Luca Baltensperger, Feeling Coerced to Consent Online (Experimental Design)

As per Article 6(1)(a) of the General Data Protection Regulation (GDPR), companies may rely on consent to process personal information. However, for consent to be legally valid, it must be given voluntarily (Article 4(11) GDPR). In Meta v Bundeskartellamt (July 4, 2023), the Court of Justice of the European Union held that voluntary consent necessitates dominant companies to offer users the option of using a service without consenting to non-necessary data processing, albeit for an appropriate fee. Following this judgment, Meta adjusted its policy in November 2023, offering users the option to use their platforms without consenting to non-necessary data processing for a fee of CHF 12. Users remain to have free access to the services if they consent. In this empirical study, we inquire whether individuals perceive reduced coercion within this new choice architecture. Using a vignette study, we empirically test the court's assumption that the option to pay for using social media reduces the coercive nature of consent to data processing.

12:30-13:30   **Finger Buffet Lunch**

13:30-14:15   **Nataliia Bielova & Cristiana Santos, Two Worlds Apart! Closing the Gap Between Regulating EU Consent and User Studies**

The EU ePrivacy Directive requires consent before using cookies or other tracking technologies, while the EU General Data Protection Regulation (GDPR) sets high-level and principle-based requirements for such consent to be valid. However, the translation of such requirements into concrete design interfaces for consent banners is far from straightforward. This situation has given rise to the use of manipulative tactics in user experience ("UX"), commonly known as dark patterns, which influence users' decision-making and may violate the GDPR requirements for valid consent. To address this problem, EU regulators aim to interpret GDPR requirements and to limit the design space of consent banners within their guidelines. Academic researchers from various disciplines address the same problem by performing user studies to evaluate the impact of design and dark patterns on users' decision making. Regrettably, the guidelines and user studies rarely impact each other. In this paper, we collected and analyzed 17 official guidelines of EU regulators and from the EU Data Protection Board (EDPB), as well as 11 consent-focused empirical user studies which we thoroughly studied from a User Interface ("UI") design perspective. We identified numerous gaps between consent banner designs recommended by regulators and those evaluated in user studies. By doing so, we contribute both to the regulatory discourse and to future user studies. We pinpoint EU regulatory inconsistencies and provide actionable recommendations for regulators. For academic scholars, we synthesize insights on design elements discussed by regulators requiring further user study evaluations. Finally, we recommend that EDPB and EU regulators, alongside usability, Human-Computer Interaction ("HCI"), and design researchers,

engage in transdisciplinary dialogue in order to close the gap between EU guidelines and user studies.

14:15-15:00   **Amit Zac & Stefan Bechtold, The Court Speaks, But Who Listens? Automated Compliance Review of the GDPR**

In July 2020, the European Court of Justice invalidated the EU-U.S. Privacy Shield with immediate effect ("Schrems II"). As a result, many personal data transfers from the European Union to the United States became illegal overnight. We present a unique dataset allowing us to not only observe what firms say about their behavior in privacy policies, but also how firms actually behave. Using machine-learning tools, we analyze the privacy policies of over 7,500 apps on the Spanish Google Play Store and find limited compliance with the Schrems II decision. We validate the quality of our classifier through manual inspection of privacy policies. Using tools from IT security research, we are able to observe the actual personal data traffic flows leaving apps towards the United States after Schrems II. Combining our observations on privacy policies and data traffic flows, our findings on compliance with Schrems II are sobering. A few weeks after Schrems II was decided, only 23% of the studied apps in our sample seem to comply with Schrems II, while 77% seem to violate the GDPR when contrasting their privacy policy and their actual personal data transfer. Over two years after Schrems II, the rate of compliant apps increase, yet we estimate that roughly 45% of the apps are non-compliant. We analyze the methodological challenges and limitations of the automated tools we use for our study. We examine the implications our findings have for the design and enforcement of the GDPR, and discuss how the combination of an automated analysis of contracts and of actual data traffic flows can improve our understanding on how to regulate the digital economy.

15:00-15:30   **Coffee Break**

15:30-16:15   **Verena Zimmermann & Lorin Schöni, Nudging Towards Informed Consent?**

Abstract: Nudges can be described as small adaptions of a choice architecture supposed to encourage users to choose the "wise" option without limiting the original choice set. In the digital domain, they can successfully support users in making secure and privacy-friendly choices. Nudges work by making use of automatic cognitive processes such as biases and primarily target automated decision making, i.e. users might not always be aware of the influence of the nudge. The talk provides an outlook on the possible use of digital nudges not to encourage a certain choice but to support informed decision-making as suggested by current data protection regulations.

16:15-17:00   **Open session – The Future of Privacy Laws in Europe, Research and Policy**

Participants

Last Name	First Name	Institution	Contact
Baltensperger	Luca	ETH Zurich	luca.baltensperger@gess.ethz.ch
Basin	David	ETH Zurich	basin@inf.ethz.ch
Bechtold	Stefan	ETH Zurich	sbechtold@ethz.ch
Bielova	Nataliia	INRIA	nataliia.bielova@inria.fr
Bouhoula	Ahmed	ETH Zurich	ahmed.bouhoula@inf.ethz.ch
Cho	Eunjung	ETH Zurich	eunjung.cho@gess.ethz.ch
De Haro	Raquel	ETH Zurich	raquel.deharo@gess.ethz.ch
Hublet	François	ETH Zurich	francois.hublet@inf.ethz.ch
Kubicek	Karel	ETH Zurich	karel.kubicek@inf.ethz.ch
Lancieri	Filippo	ETH Zurich	filippo.lancieri@gess.ethz.ch
Merane	Jakob	ETH Zurich	jakob.merane@gess.ethz.ch
Nguyen	Hoang	ETH Zurich	hoang.nguyen@inf.ethz.ch
Santos	Cristiana	Utrecht University	c.teixeirasantos@uu.nl
Schöni	Lorin	ETH Zurich	lorin.schoeni@gess.ethz.ch
Zac	Amit	ETH Zurich	amit.zac@gess.ethz.ch
Zimmermann	Verena	ETH Zurich	verena.zimmermann@gess.ethz.ch