Data Protection and Consenting Communication Mechanisms: Current Open Proposals and Challenges — Presentation

Human, Soheil; Pandit, Harshvardhan J.; Morel, Victor Pierre; Santos, Cristiana; Degeling, Martin; Rossi, Arianna; Botes, Wilhelmina; Jesus, Vitor; Kamara, Irene

Data Protection and Consenting Communication Mechanisms: Current Open Proposals and Challenges

Soheil Human, Harshvardhan J. Pandit, Victor Pierre Morel and Cristiana Santos,
Martin Degeling, Arianna Rossi, Wilhelmina Botes, Vitor Jesus, Irene Kamara

2022 International Workshop on Privacy Engineering – IWPE'22,
Co-located with 7th IEEE European Symposium on Security and Privacy
June 2022

https://doi.org/10.1109/EuroSPW55150.2022.00029

Cite as:
Soheil Human, Harshvardhan J. Pandit, Victor Pierre Morel and Cristiana Santos, Martin Degeling, Arianna Rossi, Wilhelmina Botes, Vitor Jesus, Irene Kamara (2022), "Data Protection and Consenting Communication Mechanisms: Current Open Proposals and Challenges," 2022 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), pp. 231-239, doi: 10.1109/EuroSPW55150.2022.00029.

Background

https://doi.org/10.1109/EuroSPW55150.2022.00029

Background

The Challenges of Personal Data Protection and Consenting

https://doi.org/10.1109/EuroSPW55150.2022.00029

Background

The Challenges of Personal Data Protection and Consenting

https://doi.org/10.1109/EuroSPW55150.2022.00029

Background

https://doi.org/10.1109/EuroSPW55150.2022.00029

Background

Data Protection and Consenting Communication Mechanisms (DPCCMs)

https://doi.org/10.1109/EuroSPW55150.2022.00029

Background

Data Protection and Consenting Communication Mechanisms (DPCCMs)

Privacy Signals ?

https://doi.org/10.1109/EuroSPW55150.2022.00029

Background

Data Protection and Consenting Communication Mechanisms (DPCCMs)

Privacy Signals ?

Binary “Signals”

Do Not Track (DNT)
Global Privacy Control (GPC)

https://doi.org/10.1109/EuroSPW55150.2022.00029

Background

Data Protection and Consenting Communication Mechanisms (DPCCMs)

Privacy Signals ?

Binary "Signals"

Do Not Track (DNT)

Global Privacy Control (GPC)

More Advanced/Expressive Mechanisms

the Platform for Privacy Preferences Project (P3P)

Advanced Data Protection Control (ADPC)

industry controlled efforts such as *the IAB Europe Transparency and Consent Framework7 (TCF v2)*

https://doi.org/10.1109/EuroSPW55150.2022.00029

Current Open Proposals

https://doi.org/10.1109/EuroSPW55150.2022.00029

Current Open Proposals

https://doi.org/10.1109/EuroSPW55150.2022.00029

Current Open Proposals

https://doi.org/10.1109/EuroSPW55150.2022.00029

Research Questions

https://doi.org/10.1109/EuroSPW55150.2022.00029

Research Questions

RQ1:

What are the technical factors that can be used to characterize and compare DPCCMs?

https://doi.org/10.1109/EuroSPW55150.2022.00029

Research Questions

RQ1:

What are the technical factors that can be used to characterize and compare DPCCMs?

RQ2:

What are the differences between the current open-standard DPCCM proposals (GPC and ADPC) based on the identified technical factors?

https://doi.org/10.1109/EuroSPW55150.2022.00029

Research Questions

RQ1:

What are the technical factors that can be used to characterize and compare DPCCMs?

RQ2:

What are the differences between the current open-standard DPCCM proposals (GPC and ADPC) based on the identified technical factors?

RQ3:

What are the challenges to realize a Human-centric, Accountable, Lawful, and Ethical DPCCM?

https://doi.org/10.1109/EuroSPW55150.2022.00029

Research Questions

RQ1:

What are the technical factors that can be used to characterize and compare DPCCMs?

RQ2:

What are the differences between the current open-standard DPCCM proposals (GPC and ADPC) based on the identified technical factors?

RQ3:

What are the challenges to realize a Human-centric, Accountable, Lawful, and Ethical DPCCM?

RQ4:

To what extent are the identified challenges addressed in the current GPC and ADPC proposals?

https://doi.org/10.1109/EuroSPW55150.2022.00029

Methodology

https://doi.org/10.1109/EuroSPW55150.2022.00029

Methodology

https://doi.org/10.1109/EuroSPW55150.2022.00029

Technical Factors

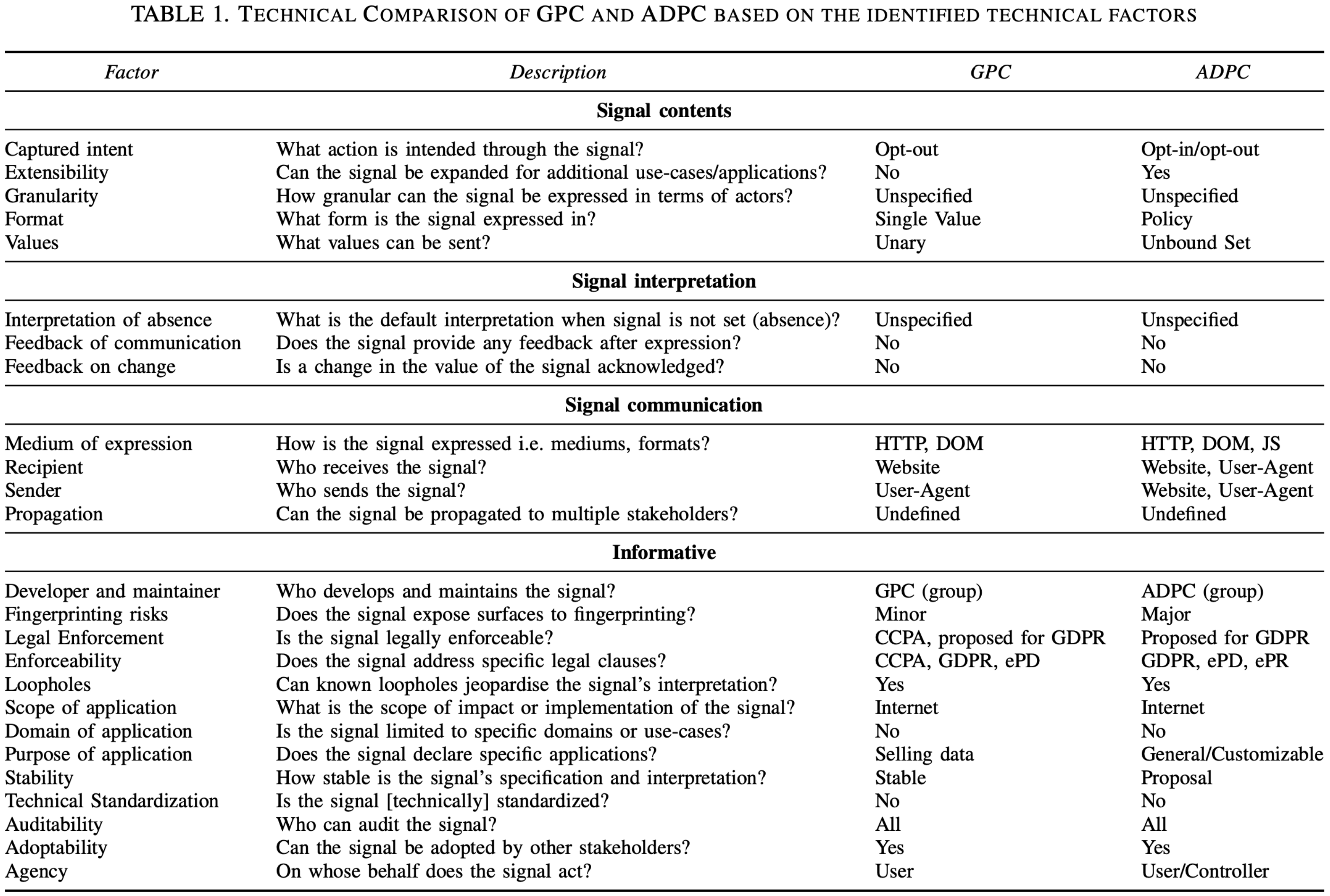


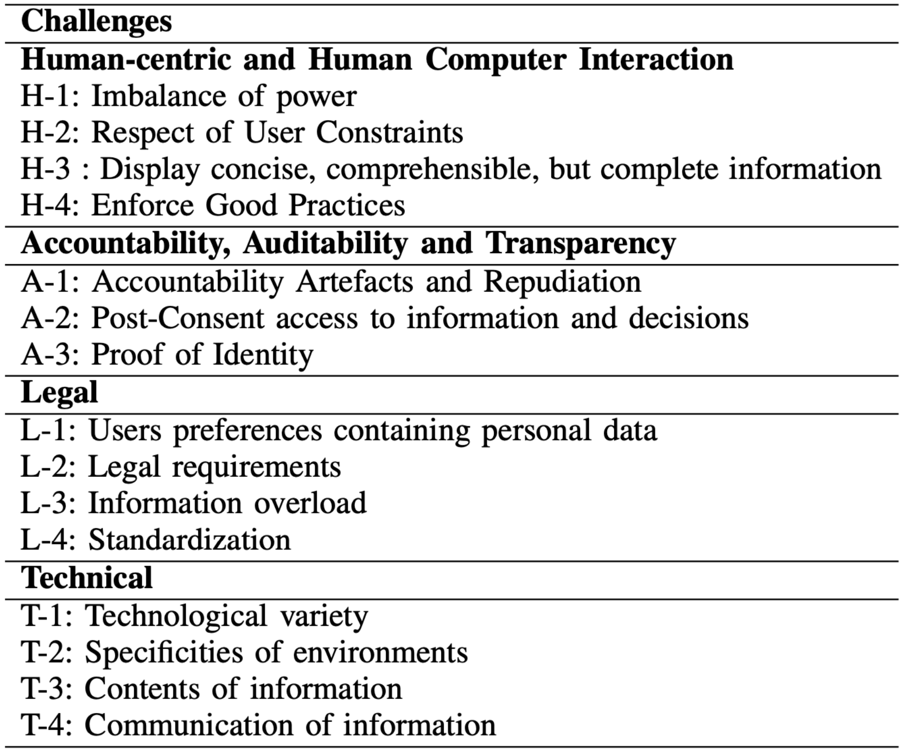
TABLE 1. Technical Comparison of GPC and ADPC based on the identified technical factors

Factor	*Description*	*GPC*	*ADPC*
Signal contents			
Captured intent	What action is intended through the signal?	Opt-out	Opt-in/opt-out
Extensibility	Can the signal be expanded for additional use-cases/applications?	No	Yes
Granularity	How granular can the signal be expressed in terms of actors?	Unspecified	Unspecified
Format	What form is the signal expressed in?	Single Value	Policy
Values	What values can be sent?	Unary	Unbound Set
Signal interpretation			
Interpretation of absence	What is the default interpretation when signal is not set (absence)?	Unspecified	Unspecified
Feedback of communication	Does the signal provide any feedback after expression?	No	No
Feedback on change	Is a change in the value of the signal acknowledged?	No	No
Signal communication			
Medium of expression	How is the signal expressed i.e. mediums, formats?	HTTP, DOM	HTTP, DOM, JS
Recipient	Who receives the signal?	Website	Website, User-Agent
Sender	Who sends the signal?	User-Agent	Website, User-Agent
Propagation	Can the signal be propagated to multiple stakeholders?	Undefined	Undefined
Informative			
Developer and maintainer	Who develops and maintains the signal?	GPC (group)	ADPC (group)
Fingerprinting risks	Does the signal expose surfaces to fingerprinting?	Minor	Major
Legal Enforcement	Is the signal legally enforceable?	CCPA, proposed for GDPR	Proposed for GDPR
Enforceability	Does the signal address specific legal clauses?	CCPA, GDPR, ePD	GDPR, ePD, ePR
Loopholes	Can known loopholes jeopardise the signal's interpretation?	Yes	Yes
Scope of application	What is the scope of impact or implementation of the signal?	Internet	Internet
Domain of application	Is the signal limited to specific domains or use-cases?	No	No
Purpose of application	Does the signal declare specific applications?	Selling data	General/Customizable
Stability	How stable is the signal's specification and interpretation?	Stable	Proposal
Technical Standardization	Is the signal [technically] standardized?	No	No
Auditability	Who can audit the signal?	All	All
Adoptability	Can the signal be adopted by other stakeholders?	Yes	Yes
Agency	On whose behalf does the signal act?	User	User/Controller

https://doi.org/10.1109/EuroSPW55150.2022.00029

Challenges

TABLE 2. MAIN CHALLENGES OF DPCCMS



Challenges
Human-centric and Human Computer Interaction
H-1: Imbalance of power
H-2: Respect of User Constraints
H-3 : Display concise, comprehensible, but complete information
H-4: Enforce Good Practices
Accountability, Auditability and Transparency
A-1: Accountability Artefacts and Repudiation
A-2: Post-Consent access to information and decisions
A-3: Proof of Identity
Legal
L-1: Users preferences containing personal data
L-2: Legal requirements
L-3: Information overload
L-4: Standardization
Technical
T-1: Technological variety
T-2: Specificities of environments
T-3: Contents of information
T-4: Communication of information

https://doi.org/10.1109/EuroSPW55150.2022.00029

Human-centric and HCI Challenges

https://doi.org/10.1109/EuroSPW55150.2022.00029

Human-centric and HCI Challenges

Imbalance of power

https://doi.org/10.1109/EuroSPW55150.2022.00029

Human-centric and HCI Challenges

Imbalance of power

Respect User Constraints

https://doi.org/10.1109/EuroSPW55150.2022.00029

Human-centric and HCI Challenges

Imbalance of power

Respect User Constraints

Display concise, comprehensible, but complete information

https://doi.org/10.1109/EuroSPW55150.2022.00029

Human-centric and HCI Challenges

Imbalance of power

Respect User Constraints

Display concise, comprehensible, but complete information

Enforce Good Practices

https://doi.org/10.1109/EuroSPW55150.2022.00029

Human-centric and HCI Challenges

GLOBAL PRIVACY CONTROL

Advanced
Data Protection
Control

Imbalance of power

Respect User Constraints

Display concise, comprehensible, but complete information

Enforce Good Practices

https://doi.org/10.1109/EuroSPW55150.2022.00029

Accountability, Auditability and Transparency Challenges

https://doi.org/10.1109/EuroSPW55150.2022.00029

Accountability, Auditability and Transparency Challenges

Accountability Artefacts and Repudiation

https://doi.org/10.1109/EuroSPW55150.2022.00029

Accountability, Auditability and Transparency Challenges

Accountability Artefacts and Repudiation

Post-Consent access to information and decisions

https://doi.org/10.1109/EuroSPW55150.2022.00029

Accountability, Auditability and Transparency Challenges

Accountability Artefacts and Repudiation

Post-Consent access to information and decisions

Proof of Identity

https://doi.org/10.1109/EuroSPW55150.2022.00029

Accountability, Auditability and Transparency Challenges

GLOBAL PRIVACY CONTROL

Advanced Data Protection Control ADPC

Accountability Artefacts and Repudiation

Post-Consent access to information and decisions

Proof of Identity

https://doi.org/10.1109/EuroSPW55150.2022.00029

Legal Challenges

https://doi.org/10.1109/EuroSPW55150.2022.00029

Legal Challenges

Users preferences containing personal data

https://doi.org/10.1109/EuroSPW55150.2022.00029

Legal Challenges

Users preferences containing personal data

Legal requirements

https://doi.org/10.1109/EuroSPW55150.2022.00029

Legal Challenges

Users preferences containing personal data

Legal requirements

Information overload

https://doi.org/10.1109/EuroSPW55150.2022.00029

Legal Challenges

Users preferences containing personal data

Legal requirements

Information overload

Standardization

https://doi.org/10.1109/EuroSPW55150.2022.00029

Legal Challenges

GLOBAL PRIVACY CONTROL

Advanced Data Protection Control ADPC

Users preferences containing personal data

Legal requirements

Information overload

Standardization

https://doi.org/10.1109/EuroSPW55150.2022.00029

Technical Challenges

https://doi.org/10.1109/EuroSPW55150.2022.00029

Technical Challenges

Technological variety

https://doi.org/10.1109/EuroSPW55150.2022.00029

Technical Challenges

Technological variety

Specificities of environments

https://doi.org/10.1109/EuroSPW55150.2022.00029

Technical Challenges

Technological variety

Specificities of environments

Contents of information

https://doi.org/10.1109/EuroSPW55150.2022.00029

Technical Challenges

Technological variety

Specificities of environments

Contents of information

Communication of information

https://doi.org/10.1109/EuroSPW55150.2022.00029

Technical Challenges

GLOBAL PRIVACY CONTROL

Advanced
Data Protection
Control
ADPC

Technological variety

Specificities of environments

Contents of information

Communication of information

https://doi.org/10.1109/EuroSPW55150.2022.00029

Conclusion

https://doi.org/10.1109/EuroSPW55150.2022.00029

Conclusion

Many other interconnected challenges

https://doi.org/10.1109/EuroSPW55150.2022.00029

Conclusion

Many other interconnected challenges

Opt-in vs. Opt-out

https://doi.org/10.1109/EuroSPW55150.2022.00029

Conclusion

Many other interconnected challenges

Opt-in vs. Opt-out

Minimal (Binary) vs. Advanced (Expressive)

https://doi.org/10.1109/EuroSPW55150.2022.00029

Conclusion

Many other interconnected challenges

Opt-in vs. Opt-out

Minimal (Binary) vs. Advanced (Expressive)

Top-down vs. Bottom-up Realisation/Enforcement

https://doi.org/10.1109/EuroSPW55150.2022.00029

Conclusion

Many other interconnected challenges

Opt-in vs. Opt-out

Minimal (Binary) vs. Advanced (Expressive)

Top-down vs. Bottom-up Realisation/Enforcement

https://doi.org/10.1109/EuroSPW55150.2022.00029

Bibliography

[1] H. Smith, T. Dinev, and H. Xu, “Information Privacy Research: An Interdisciplinary Review,” MIS Quarterly, vol. 35, pp. 989–1015, Dec. 2011.

[2] C. M. Gray, C. Santos, N. Bielova, M. Toth, and D. Clifford, “Dark Patterns and the Legal Requirements of Consent Banners: An Interaction Criticism Perspective,” in Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems, ser. CHI ’21. New York, NY, USA: Association for Computing Machinery, May 2021, pp. 1–18.

[3] A. Mathur, G. Acar, M. Friedman, E. Lucherini, J. Mayer, M. Chetty, and A. Narayanan, “Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites,” Proc. ACM Hum.-Comput. Interact., vol. 1, no. CSCW, 2019.

[4] M. Nouwens, I. Liccardi, M. Veale, D. Karger, and L. Kagal, “Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence,” arXiv:2001.02479 [cs], Jan. 2020, arXiv: 2001.02479.

[5] C. Wylie, Mindf* ck: Cambridge Analytica and the plot to break America. Random House, 2019.

[6] S. Zuboff, The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power, 1st ed. New York: PublicAffairs, Jan. 2019.

[7] S. Human, “THE HALE WHALE: A Framework for the Co-creation of Sustainable, Human-centric, Accountable, Lawful, and Ethical Digital Sociotechnical Systems,” Sustainable Computing Paper Series, no. 2022/01, 2022.

[8] S. Human and F. Cech, “A Human-Centric Perspective on Digital Consenting: The Case of GAFAM,” in Human Centred Intelligent Systems, ser. Smart Innovation, Systems and Technologies, A. Zimmermann, R. J. Howlett, and L. C. Jain, Eds. Singapore: Springer, 2021, pp. 139–159.

[9] S. Human, R. Alt, H. Habibnia, and G. Neumann, “Human-centric Personal Data Protection and Consenting Assistant Systems: Towards a Sustainable Digital Economy,” in Proceedings of the 55th Hawaii International Conference on System Sciences. Hawaii, USA: University of Hawaii, 2022, pp. 4727–4736.

[10] S. Human and M. Kazzazi, “Contextuality and intersectionality of e-consent: A human-centric reflection on digital consenting in the emerging genetic data markets,” in 2021 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW). IEEE, 2021, pp. 307–311.

[11] S. Zimmeck and K. Alicki, “Standardizing and implementing do not sell,” in Proceedings of the 19th Workshop on Privacy in the Electronic Society, 2020, pp. 15–20.

[12] S. Human, M. Schrems, A. Toner, Gerben, and B. Wagner, “Advanced Data Protection Control (ADPC),” Vienna University of Economics and Business (WU Wien), Vienna, Sustainable Computing Reports and Specifications 2021/01, 2021.

[13] S. Human, “Advanced data protection control (adpc): An interdisciplinary overview,” Sustainable Computing Paper Series, no. 2022/01, 2022.

[14] M. Hils, D. W. Woods, and R. Bo¨hme, “Privacy preference signals: Past, present and future,” Proceedings on Privacy Enhancing Technologies, vol. 2021, no. 4, pp. 249–269, 2021.

[15] “Decision on the merits 21/2022 of 2 february 2022? complaint relating to transparency & consent framework,” 2022.

[16] K. Charmaz, Constructing grounded theory. sage, 2014.

[17] M. Burgess, “The tyranny of GDPR popups and the websites failing to adapt,” vol. 22, p. 2019, 2018.

[18] S. Human, G. Neumann, and M. F. Peschl, “[How] can pluralist approaches to computational cognitive modeling of human needs and values save our democracies?” Intellectica, vol. 70, pp. 165– 180, 2019.

[19] V. Ha, K. Inkpen, F. Al Shaar, and L. Hdeib, “An examination of user perception and misconception of internet cookies,” in CHI’06 Extended Abstracts on Human Factors in Computing Systems, 2006, pp. 833–838.

[20] C. Santos, A. Rossi, L. Sanchez Chamorro, K. Bongard-Blanchy, and R. Abu-Salma, “Cookie banners, what’s the purpose? analyzing cookie banner text through a legal lens,” in Proceedings of the 20th Workshop on Workshop on Privacy in the Electronic Society. ACM, 2021, p. 187–194.

[21] O. Kulyk, A. Hilt, N. Gerber, and M. Volkamer, “”This Website Uses Cookies”: Users’ Perceptions and Reactions to the Cookie Disclaimer,” in Proceedings 3rd European Workshop on Usable Security. Internet Society, 2018.

[22] N. Ebert, K. Alexander Ackermann, and B. Scheppler, “Bolder is better: Raising user awareness through salient and concise privacy notices,” in Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems, 2021, pp. 1–12.

[23] C. Utz, M. Degeling, S. Fahl, F. Schaub, and T. Holz, “(Un)informed Consent: Studying GDPR Consent Notices in the Field,” in Proc. CCS, ser. CCS ’19. New York, NY, USA: ACM, 2019, pp. 973–990.

[24] S. Human, R. Gsenger, and G. Neumann, “End-user empowerment: An interdisciplinary perspective,” in Proceedings of the 53rd Hawaii International Conference on System Sciences, Hawaii, United States, 2020, pp. 4102–4111.

[25] V. Jesus and H. J. Pandit, “Consent receipts for a usable and auditable web of personal data,” IEEE Access, pp. 1–1, 2022.

[26] V. Jesus, “Towards an accountable web of personal information: The web-of-receipts,” IEEE Access, vol. 8, pp. 25383–25394, 2020.

[27] C. Bier, K. Ku¨hne, and J. Beyerer, “Privacyinsight: The next generation privacy dashboard,” in Privacy Technologies and Policy, S. Schiffner, J. Serna, D. Ikonomou, and K. Rannenberg, Eds. Cham: Springer International Publishing, 2016, pp. 135–152.

[28] V. Jesus, “Pragmatic online privacy: the sfte approach,” in 1st Intl Workshop on Consent Management in Online Services, Networks and Things, with 6th IEEE EuroS&P, 2021.

[29] A. Acquisti, I. Adjerid, and L. Brandimarte, “Gone in 15 seconds: The limits of privacy transparency and control,” IEEE Security Privacy, vol. 11, no. 4, pp. 72–74, 2013.

[30] A. Adams. (2021-11-11) Algorithmic Decisions and Their Human Consequences — The Regulatory Review.

[31] C. Boniface, I. Fouad, N. Bielova, C. Lauradoux, and C. Santos, “Security analysis of subject access request procedures,” in Annual Privacy Forum. Springer, 2019, pp. 182–209.

[32] C. Santos, N. Bielova, and C. Matte, “Are cookie banners indeed compliant with the law? : Deciphering eu legal requirements on consent and technical means to verify compliance of cookie banners,” Technology and Regulation, vol. 2020, p. 91aˆC“135, Dec. 2020.

[33] C. Santos, M. Nouwens, M. To´th, N. Bielova, and V. Roca, “Consent management platforms under the gdpr: processors and/or controllers?” in APF, 2021.

[34] A.deprotectiondesdonne´es,“Decisiononthemerits21/2022of2 february 2022. case number: Dos-2019-01377. complaint relating to transparency & consent framework.” 2022.

[35] C. Bravo-Lillo, L. Cranor, S. Komanduri, S. Schechter, and M. Sleeper, “Harder to ignore? revisiting {Pop-Up} fatigue and approaches to prevent it,” in 10th Symposium On Usable Privacy and Security (SOUPS 2014), 2014, pp. 105–111.

[36] D. Lindegren, F. Karegar, B. Kane, and J. S. Pettersson, “An evaluation of three designs to engage users when providing their consent on smartphones,” Behaviour & Information Technology, vol. 40, no. 4, pp. 398–414, 2021.

[37] W. Melicher, M. Sharif, J. Tan, L. Bauer, M. Christodorescu, and P. G. Leon, “(do not) track me sometimes: Users’ contextual preferences for web tracking,” Proceedings on Privacy Enhancing Technologies, vol. 2016, no. 2, pp. 135–154, 2015.

[38] I. Kamara and E. Kosta, “Do Not Track initiatives: regaining the lost user control,” International Data Privacy Law, vol. 6, no. 4, pp. 276–290, 10 2016.

[39] N. C. Gleeson and I. Walden, “’it’s a jungle out there’?: Cloud computing, standards and the law,” Eur. J. Law Technol., vol. 5, 2014.

[40] J.-P. Quemard, J. Schallabok, I. Kamara, and M. Pocs, “Guidance and gap analysis for european standardisation: Privacy standards in the information security context,” 2019.

[41] A.Harcourt, G. Christou,and S. Simpson, Global Standard Setting in Internet Governance. Oxford: Oxford University Press, January 2020.

[42] KiernanandMueller,“Standardizing security: Surveillance,human rights, and the battle over tls 1.3,” Journal of Information Policy, vol. 11, p. 1, 2021.

[43] “An eu strategy on standardisation. setting global standards in support of a resilient, green and digital eu single market, communication from the commission to the european parliament, the council, the european economic and social committee and the committee of the regions com(2022) 31 final.),” 2022.

[44] P. De Hert and S. Gutwirth, “Privacy, data protection and law enforcement. opacity of the individual and transparency of power,” Privacy and the criminal law, pp. 61–104, 2006.

[45] V.Morel,M.Cunche,andD.LeMe´tayer,“Agenericinformation and consent framework for the iot,” in 2019 18th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/13th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE). IEEE, 2019, pp. 366–373.

[46] L. Demir, M. Cunche, and C. Lauradoux, “Analysing the privacy policies of Wi-Fi trackers.” ACM Press, 2014, pp. 39–44.

[47] M. Cunche, D. L. Me´tayer, and V. Morel, “Colot: a consent and information assistant for the iot,” in Proceedings of the 13th ACM Conference on Security and Privacy in Wireless and Mobile Networks, 2020, pp. 334–336.

[48] S. Giordano, V. Morel, M. O. Nen, M. Musolesi, D. Andreoletti, F. Cardoso, A. Ferrari, L. Luceri, C. Castelluccia, D. L. M. Tayer, C. V. Rompay, and B. Baron, “UPRISE-IoT: User-centric Privacy & Security in the IoT,” in SPIoT, 2019, p. 17.

[49] H. J. Pandit, A. Polleres, B. Bos, R. Brennan, B. Bruegger, F. J. Ekaputra, J. D. Ferna´ndez, R. G. Hamed, M. Lizar, E. Schlehahn, S. Steyskal, and R. Wenning, “Creating A Vocabulary for Data Privacy,” in The 18th International Conference on Ontologies, DataBases, and Applications of Semantics (ODBASE2019), Rhodes, Greece, 2019, p. 17.

https://doi.org/10.1109/EuroSPW55150.2022.00029