RESEARCH CENTRES

Inria Centre at Université Grenoble Alpes

Inria Lyon Centre

IN PARTNERSHIP WITH:

Institut national des sciences appliquées de Lyon

2023
ACTIVITY REPORT

Project-Team
PRIVATICS

Privacy Models, Architectures and Tools for the Information Society

IN COLLABORATION WITH: Centre of Innovation in Telecommunications and Integration of services

DOMAIN

Algorithmics, Programming, Software and Architecture

THEME

Security and Confidentiality

Contents

Project-Team PRIVATICS

Creation of the Project-Team: 2014 July 01

Keywords

Computer sciences and digital sciences

A1.2.5. – Internet of things

A4.8. – Privacy-enhancing technologies

A5.1.9. – User and perceptual studies

A9.9. – Distributed AI, Multi-agent

Other research topics and application domains

B6.3.1. – Web

B6.3.2. – Network protocols

B9.6.2. – Juridical science

B9.10. – Privacy

1 Team members, visitors, external collaborators

Research Scientists

- Vincent Roca [Team leader, INRIA, Researcher, HDR]
- Nataliia Bielova [INRIA, Researcher, HDR]
- Claude Castelluccia [INRIA, Senior Researcher, HDR]
- Heber Hwang Arcolezi [INRIA, ISFP, from Oct 2023]
- Cedric Lauradoux [INRIA, Researcher]
- Mohamed Maouche [INRIA, ISFP]
- Cristiana Teixeira Santos [INRIA, Starting Research Position, from Sep 2023 until Oct 2023]
- Cristiana Teixeira Santos [INRIA, Starting Research Position, from Jun 2023 until Jul 2023]

Faculty Members

- Antoine Boutet [INSA LYON, Associate Professor, from Sep 2023]
- Antoine Boutet [INSA LYON, Associate Professor Delegation, until Aug 2023]
- Mathieu Cunche [INSA LYON, Associate Professor, HDR]

Post-Doctoral Fellows

- Alexandre Lodie [INRIA, Post-Doctoral Fellow, from Mar 2023]
- Abhishek Mishra [INSA LYON, from Dec 2023]

PhD Students

- Jan Aalmoes [INSA LYON]
- Coline Boniface [UGA]
- Teodora Curelariu [UGA]
- Suzanne Lansade [INRIA, until Apr 2023]
- Thomas Lebrun [INRIA]
- Gilles Mertens [INRIA]
- Samuel Pelissier [INSA LYON]
- Michael Toth [INRIA, until May 2023]

Technical Staff

- Ivan Baheux-Blin [INRIA, Engineer, from Jun 2023]
- Julien Barnier [CNRS, Engineer, until Jul 2023]
- Adrien Baud [INRIA, Engineer, until Jan 2023]
- Mohamed Bechorfa [INRIA, Engineer, from Feb 2023]
- Nathan Brunet [INRIA, Engineer, from Feb 2023]

Interns and Apprentices

- Mohamed Bechorfa [INSA LYON, Intern, until Feb 2023]
- Gaspard Berthelier [CENTRALESUPELEC, Intern, until Jun 2023]
- Essohanam Djeki [INRIA, Intern, from Sep 2023]
- Alexandru Dodon [INRIA, Intern, from Mar 2023 until Aug 2023]
- Aicha El Bou [INSA LYON, Intern, from May 2023 until Aug 2023]
- Murielle Iradukunda [INRIA, Intern, from May 2023 until Aug 2023]

Administrative Assistant

- Helen Pouchot-Rouge-Blanc [INRIA]

External Collaborator

- Colin Gray [UNIV PURDUE - INDIANA, from May 2023 until May 2023]

2 Overall objectives

2.1 Context and overall objectives

From ambient privacy to massive and ubiquitous data collection: In an very short span of time, we switched from a world where "ambient privacy" was the rule, to a situation dominated by massive, ubiquitous and precise data collections, where trying to protect our privacy requires constant efforts. If, 50 years ago, the perceived threat was that of an *state surveillance* (e.g., the SAFARI project led to the creation in 1978 of the French privacy regulation and the DPA, CNIL), nowadays, *"capitalism surveillance"*, a term popularized by Shoshana Zubboff, is a concern of equal, if not greater, importance. It has been made possible by the super-fast development of the Web in the 1990s, of smartphones ten years later, and now of IoT devices of all kinds, and all these technological breakthroughs led to the creation of highly profitable giant companies, most of which leverage on user-data for profiling and targeting.

Undoubtedly, this digital world opened major opportunities, highly beneficial to the society in general and to individuals in particular. However, it also poses considerable privacy threats that can potentially turn these new technologies into a nightmare if they are not accompanied by appropriate legal and ethical rules. As the French "Loi Informatique et Liberté" (1978) says in its first chapter: "Information technology must be at the service of every citizen. [...] It must not infringe on human identity, human rights, privacy, or personal or public freedom."

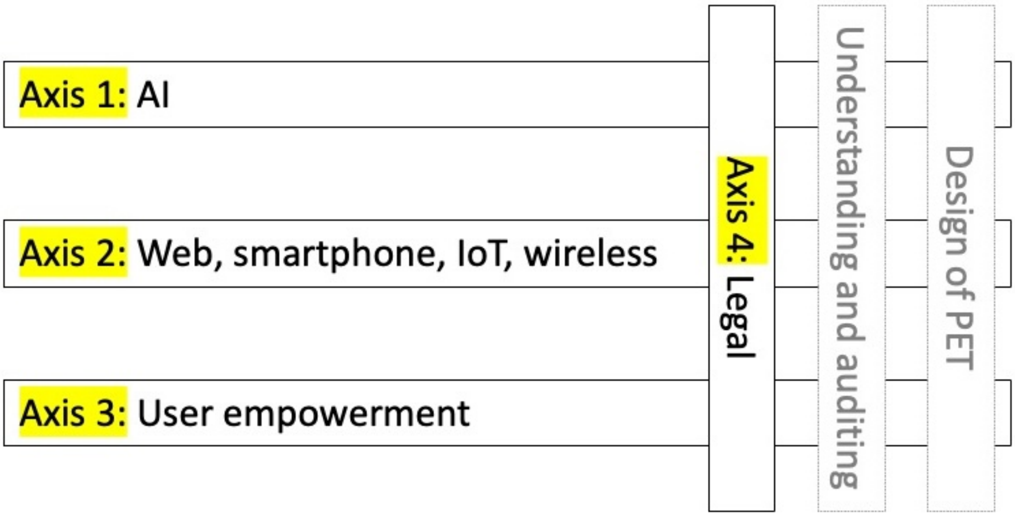
Making the world – a little bit – better: Privacy is thus essential to protect individuals, for instance against potential misuses of personal data. Privacy is also essential to protect the society, as has been highlighted by the misuse of personal data in order to surreptitiously influence voters in elections (e.g., Cambridge Analytica). But privacy is too important to be left only in the hands of individuals: the role of regulators and Data Protection Authorities is fundamental from this viewpoint, leading to regulations (e.g., GDPR) that protect all citizens by default.

In this landscape, public research has a key role to play. By working in a complementary manner, from highly theoretical subjects up to the reverse engineering of deployed systems, or the design of privacy enhancing technologies, public research also contributes to making the world – a little bit – better.

3 Research program

PRIVATICS activities: Since its creation in 2014, the PRIVATICS team focuses on privacy protection in this digital world, and its members contribute to the domain through theoretical, practical, but also transdisciplinary activities. Indeed, while the team mainly focuses on technical aspects of privacy, the team also interacts with legal, economical dimension of privacy. In order to be impactful, for our research community but also for the society, the approach followed is fundamentally transdisciplinary. It covers the computer-science, legal and design domains, with sometimes sociological contributions, by the means of enriched collaborations with the members of these disciplines.

4 Application domains


Axis 1: AI
Axis 2: Web, smartphone, IoT, wireless
Axis 3: User empowerment
Axis 4: Legal
Understanding and auditing
Design of PET

More specifically, our activities cover four main research axes, depicted above, namely:

1. the **"AI" research** axis includes works on "privacy considerations in ML" (e.g., Federated ML and the explainability of Automated Decision Systems), but also on the "use of ML for privacy" (e.g., for medical report anonymisation);

2. the **"Web, smartphone, IoT and wireless networks"** (e.g., BLE and LoRaWAN) research axis focuses on several types of connected devices and services, responsible of major data leaks, for which our contributions can be highly impactful. We conducted large scale measurements, we reverse-engineered several technologies, and we proposed Privacy Enhancement Technologies (PET) when appropriate;

3. the **"User Empowerment"** research axis studies how users keep control over their data and how they are being manipulated. For example, this axis involves large-scale measurement of consent on the Web (in form of cookie banners), dark patterns that manipulate users' decision making when interacting with consent, and tensions with legal requirements for GDPR consent when designing consent banners – this axes is particularly advanced, at the intersection with the "Legal" axis presented below.

4. the **"Legal"** research axis intersects all previous axes, and consists in transdisciplinary research in Computer Science and Law. We analyze *legal requirements for compliance with the EU Data Protection Laws* of systems and services, such as cookie banners, providers of such banners and their legal roles and responsibilities (e.g., we refined legal high-level requirements into concrete system requirements, such as 22 low-level requirements to assess compliance of consent banners). We also analyze the technical and regulation aspects of privacy invasive technologies that present significant risks (e.g., face recognition, or intelligent surveillance cameras). In front of such complex problems

having both technical and legal dimensions, advances are only possible through a transdisciplinary work with legal scholars.

Across these topics, we work on:

- the analysis of systems and services in order to *understand them, sometimes to audit them* (e.g., by measuring personal data leaks through large scale measurement campaigns);
- the design of privacy enhancement technologies (PET), in various domains (e.g., to reduce privacy risks in wireless technologies, or to enhance privacy properties of Federated ML).

Transdisciplinarity made concrete: Privacy being fundamentally at the crossroad of several domains, many hard research questions that we address in the previous four research axes, require a transdisciplinary approach, where experts of different domains share their expertise and benefit from one another. This is the approach we deliberately chose. Therefore, PRIVATICS works with scholars in the legal, economist, design, and social science domains. It takes various forms: participation to common funded projects (e.g., the IPoP and CovOMM projects), participation to common research activities, co-direction of legal PhDs, recruitment of a legal Post-Doctorate, recruitment of an Inria International Chair Junior, and publications in legal venues. PRIVATICS makes transdisciplinarity concrete.

5 Social and environmental responsibility

5.1 Environmental impacts of research results

The activities of PRIVATICS are not directly related to environmental considerations. However, promoting privacy in a connected world advocates for less data collection and processing, as opposed to massive data collection and big data (e.g., in the case of Internet of Things systems). From this point of view, we believe that our research results are aligned with environmental considerations.

5.2 Societal impacts of research results

Collaborating with regulators thanks to our independent expertise: Developing an *independent expertise* is part of our values. Although big tech companies, such as GAFA, contribute to several privacy enhancing technologies (e.g., in the AI domain) and can offer funding opportunities, we chose not to go into that direction.

We believe that the most efficient way to combat the "surveillance capitalism" doctrine these companies created is to work with regulators. France since 1978 with the "Loi Informatique et Liberté", the EU with the privacy regulation (GDPR, ePrivacy, DMA/DSA) during the past years, and now with AI regulation, paved the way for a better world, more respectful of the individual human rights, internationally. We contribute concretely to this trend.

Since the beginning, PRIVATICS works closely with the French Data Protection Agency, CNIL. During the period, it took the form of a temporary leave to CNIL for Nataliia Bielova, the nomination of Claude Castelluccia as a CNIL commissioner, the participation of CNIL in the IOTics and now IPoP projects, and feedback to several CNIL and EDPB public consultations. Our work is also cited in legal decisions (Belgian DPA). Additionally, several PRIVATICS members are experts for ENISA (Claude Castelluccia and Cédric Lauradoux), member of ENISA Data Protection Engineering Working Group (Claude Castelluccia) and EDPB (Mathieu Cunche, Nataliia Bielova). We contributed to several landmark reports on these topics.

We believe that PRIVATICS successfully helped regulators during this period, bringing our expertise at various levels in various ways. We think this is the best approach to be impactful, in particular with respect to giant Internet companies whose business model is so profitable that they have little incentives to change it, unless obliged to do so.

Contributing to the establishment of doctrines regarding technologies that can have major societal impacts: Certain new technologies raise major questions, with societal and ethical potential implications. We contributed to the establishment of doctrines through reports on AI regulation, facial recognition regulation. The major involvement of Claude Castelluccia in the CNIL Board enabled to contribute to the French DPA doctrine with respect to various important subjects related to new technologies. Being in position to influence public doctrines, independently of any private interest, following a scientific approach, is part of the major outcomes of our team.

Transfer to well chosen private companies and public administrations: Our decision not to work with GAFA does not imply we do not work with private companies. We have two future CIFRE PhD with small French companies in the domain of online, sovereign identity management, and "de-googleized" operating system for smartphones. We have several projects with public hospitals and administrations. We provided technical expertise (under confidentiality clauses) on data protection for Europol, the French and German ministry of the interior about the implementation of the EPRIS framework in the proposal for a regulation on automated data exchange for police cooperation ("Prüm II"). Those collaborations open the way for concrete and mutually beneficial transfers, in line with our values.

Contributing to international standards: Being able to contribute to standards in order to promote our views and research outputs, is a highly efficient manner to have concrete impacts. One of us did it for privacy extensions of IEEE 802 standards and was officially recognized for his expertise. In a totally different domain, another one co-chaired an IETF group and published 15 RFCs, including 1 in 2023.

Actions towards the general public: Scientific outreach towards the general public is one of our missions, and we significantly contributed. The MOOC on privacy in the digital world attracted a bit more than 40,000 persons, has been qualified "of public interest" by one of the participants. It is one example. Additionally, every year we contribute to the "Fête de la Science" by proposing mini-conferences and working sessions with the young public, one of us regularly goes into high school to promote science and privacy, we participate also to conferences with non-scientific public and we are interviewed by journalists. We take it to heart to "vulgarize" and help our fellow citizens understand this highly complex domain, with so many societal implications. Although we sometimes would like to do more, this is time consuming and we try to find a good balance.

Actions in support of public authorities: In addition to working with regulators (see above), helping public authorities is also part of our missions. We did it during the COVID19 crisis, and our decisive work on contact and presence tracing protocols, in the context of the public/private StopCovid project-team, contributed to a successful "crisis application". We also contributed, with all the member of this StopCovid project-team, to strengthen the technological and digital sovereignty of the Nation, with a solution focused on the health authority, respectful of our values and choices.

Participation in ethical committees: Additionally, several PRIVATICS members are part of various ethical committees:

- Vincent Roca is member of the Inria COERLE (commité d'évaluation des risques légaux et éthiques);

- Cédric Lauradoux represents the Inria COERLE (commité d'évaluation des risques légaux et éthiques) in the Grenoble research center, helping local researchers to fill in their application form;
- Cédric Lauradoux is member of the University of Grenoble Alps (UGA) ethical committee;
- Mathieu Cunche is member of *Comité d'éthique de la recherche (CER)* of Lyon University.

6 Highlights of the year

6.1 Awards

Nataliia Bielova - W@Privacy "Rising Star" - November 2023 Nataliia won the W@Privacy Awards, "Rising Star" category, recognizing a professional with less than ten years of experience in the privacy field who has demonstrated promising technical or practical abilities through work and/or academic research on privacy topics.

Best paper, SECRYPT 20th Int. Conference on Security and Communications, 2023. The "RSSI-based Fingerprinting of Bluetooth Low Energy Devices" publication, co-authored by Mathieu Cunche, received the SECRYPT 2023 best paper award. Related publication: [9]

Student Paper Award Honorable Mention, 2023. The article: "My Cookie is a phoenix: detection, measurement, and lawfulness of cookie respawning with browser fingerprinting", co-authored by Nataliia Bielova and Imane Fouad, published at PoPETS 2022, received the Future of Privacy Forum's Privacy Papers for Policymakers, Student Paper Award Honorable Mention.

7 New software, platforms, open data

7.1 New software

7.1.1 PRESERVE

Name: PRESERVE, a web platform to raise awareness of privacy issues

Keywords: Privacy, Geolocation

Functional Description: This platform aims to raise users' awareness of privacy issues. It implements tools in order to inspect location history, like [https://hal.inria.fr/hal-02421828] where a user is able to inspect the private and sensitive information inferred from its own location data.

Authors: Antoine Boutet, Adrien Baud

Contact: Antoine Boutet

7.1.2 NLP Privacy

Name: NLP Privacy

Keywords: Privacy, Natural language processing

Scientific Description: Associated publication: G. BERTHELIER, A. BOUTET, A. RICHARD, "Toward training NLP models to take into account privacy leakages", in : BigData 2023 - IEEE International Conference on Big Data, IEEE, p. 1–9, Sorrento, Italy, December 2023, [hal:hal-04299405].

Functional Description: This library provides tools to evaluate three privacy risks on NLP models trained on sensitive data: 1) the counterfactual memorization, which corresponds to rare and sensitive information which has too much influence on the model, 2) the membership inference, and 3) the ability to extract verbatim training data from models.

Authors: Antoine Boutet, Gaspard Berthelier

Contact: Antoine Boutet

8 New results

8.1 Research axis 1: AI

8.1.1 Toward training NLP models to take into account privacy leakages

Participants: Gaspard Berthelier, Antoine Boutet.

With the rise of machine learning and data-driven models especially in the field of Natural Language Processing (NLP), a strong demand for sharing data between organisations has emerged. However datasets are usually composed of personal data and thus subject to numerous regulations which require anonymization before disseminating the data. In the medical domain for instance, patient records are extremely sensitive and private, but the de-identification of medical documents is a complex task. Recent advances in NLP models have shown encouraging results in this field, but the question of whether deploying such models is safe remains. In this paper, we evaluate three privacy risks on NLP models trained on sensitive data. Specifically, we evaluate counterfactual memorization, which corresponds to rare and sensitive information which has too much influence on the model. We also evaluate membership inference as well as the ability to extract verbatim training data from the model. With this evaluation, we can cure data at risk from the training data and calibrate hyper parameters to provide a supplementary utility and privacy tradeoff to the usual mitigation strategies such as using differential privacy. We exhaustively illustrate the privacy leakage of NLP models through a use-case using medical texts and discuss the impact of both the proposed methodology and mitigation schemes.

Related publication: [7]

8.1.2 Towards an evolution in the characterization of the risk of re-identification of medical images

Participants: Antoine Boutet, Mohamed Maouche, et al..

As facial recognition technology proliferates, concerns emerge regarding its application to medical imaging, specifically Magnetic Resonance Imaging (MRI). This paper investigates privacy risks associated with MRI data, including reidentification through social network photographs and sensitive attribute inference. The exponential growth in MRI quality coincides with the increasing sophistication of facial recognition tools, raising the potential for re-identification using medical images. Our attack involves reconstructing faces and applying facial recognition techniques to extract identifying features that can be compared to photographs. Legal frameworks like GDPR mandate the assessment and protection of personal data, necessitating continuous risk evaluation. Beyond re-identification, we explore the inference of individual attributes from MRI images, such as age, gender, and ethnic group. This research assesses the privacy risks associated with MRI data by taking into account the evolution of facial recognition and reconstruction tools that have become increasingly accessible. We also show that facial hair removal technique on photographs increases the risk of re-identification. Overall, our results highlight vulnerabilities in sharing MRI data, emphasizing the need for enhanced privacy safeguards.

Related publication: [8]

8.2 Research axis 2: Web, smartphone, IoT, and wireless

8.2.1 RSSI-based Fingerprinting of Bluetooth Low Energy Devices

Participants: Mathieu Cunche, et al..

To prevent tracking, the Bluetooth Low Energy protocol integrates privacy mechanisms such as address randomization. However, as highlighted by previous researches address randomization is not a silver bullet and can be circumvented by exploiting other types of information disclosed by the protocol such as counters or timing. In this work, we propose a novel attack to break address randomization in BLE exploiting side information that has not been considered before: Received Signal Strength Indication (RSSI). More precisely, we demonstrate how RSSI measurements, extracted from received BLE advertising packets, can be used to link together the traces emitted by the same device or re-identify it despite address randomization. The proposed attack leverages the distribution of RSSI to create a fingerprint of devices. An empirical evaluation of the attack on various scenarios demonstrate its effectiveness. For instance in the static context, in which devices remain at the same position, the proposed approach yields a re-identification accuracy of up to 99%, which can even be boosted by increasing the number of receivers controlled by the adversary.

Related publication: [9]

8.2.2 PEPPER: Precise Privacy-Preserving Contact Tracing with Cheap, BLE/UWB Capable Tokens

Participants: Vincent Roca, Mathieu Cunche, Antoine Boutet, et al..

Contact Tracing (CT) is an old, recognized epidemiological tool, and since a digital variant is now within reach, a variety of smartphone-based solutions have been rapidly developed and deployed since 2020, with mixed results and amid controversies. Yet, achieving reliable and effective digital CT at large scale is still an open problem. In this work, we contribute with an open source software platform on top of which various CT solutions can be quickly developed and tested. More specifically, we design PEPPER, which jointly leverages Bluetooth Low Energy (BLE) and Ultra Wide Band (UWB) radios for contact detection, combined with the DESIRE privacy-preserving CT protocol. We show that PEPPER+DESIRE can operate on cheap physical tokens based on low-power microcontrollers, opening new use-cases with less personal, potentially disposable devices, that could be more widely used. We also evaluate the complementarity of Bluetooth and UWB in this context, via experiments mimicking various scenarios relevant for CT. Compared to BLE-only CT, we show that UWB can decrease false negatives (e.g., in presence of human body occlusion), meaning that more actual contacts will be found, a key benefit from an epidemiological viewpoint. Our results suggest that, while PEPPER+DESIRE improves precision over state-of-the-art, further research is required to harness UWB-BLE synergy for CT in practice. To this end, our open source platform (which can run on an open-access testbed) provides a useful playground for the research community.

Related publication: [10]

8.2.3 COVoM : Covid On My Mobile: To what extent Contact-Tracing Apps become a tool in policy-makers' and citizens' hands?

Participants: Vincent Roca, et al..

A comparative and pragmatic study on contact tracing applications from intention to implementation, and test by use: France, Japan and Colorado. More than any other crisis, the COVID19 pandemic has required the articulation of public policies in different fields, and with individual as well as collective behaviors. Considered as a passage point to support public health institutions and complete traditional epidemiological tools, digital contact tracing using smartphones has been a core innovation in response to the COVID-19 pandemic. Designed, developed, and put into service quickly, with many corrections made during the stage of final use by the citizens, this innovation opened debates regarding trust and privacy issues, both essential to its efficiency. Through a pragmatic approach, the COVoM project proposes an international comparative study of the strategies of public actors' and of the attitude of the citizens vis-à-vis CTAs, with focus on the different "adoption" trajectories, from the phases of intention, conception to final stage of implementation and use. The goal is to understand to what extent government choices can shape the citizens' decision to use or not such a health digital tool. The project will help policy makers, app designers, prevention operators, and professionals to identify the conditions under which digitalizing contact tracing can be relevant to the fight against pandemics.

The COVoM research offers the premises and the database to explore fundamental questions concerning the relationship of individuals to contamination risks. It also contributes to the sociology of public action digitalization and to the "crisis" innovation studies.

Related publication: [18]

8.2.4 I-GWAS: Privacy-Preserving Interdependent Genome-Wide Association Studies

Participants: Antoine Boutet, et al..

Genome-wide Association Studies (GWASes) identify genomic variations that are statistically associated with a trait, such as a disease, in a group of individuals. Unfortunately, careless sharing of GWAS statistics might give rise to privacy attacks. Several works attempted to reconcile secure processing with privacy-preserving releases of GWASes. However, we highlight that these approaches remain vulnerable if GWASes utilize overlapping sets of individuals and genomic variations. In such conditions, we show that even when relying on state-of-the-art techniques for protecting releases, an adversary could reconstruct the genomic variations of up to 28.6% of participants, and that the released statistics of up to 92.3% of the genomic variations would enable membership inference attacks. We introduce I-GWAS, a novel framework that securely computes and releases the results of multiple possibly interdependent GWASes. I-GWAS continuously releases privacy-preserving and noise-free GWAS results as new genomes become available.

Related publication: [12]

8.3 Research axis 3: User empowerment

8.3.1 The Effect of Design Patterns on (Present and Future) Cookie Consent Decisions: Supplemental Materials

Participants: Nataliia Bielova, et al..

This document provides supplemental materials directly cited in the proceedings of the USENIX Security Symposium 2024 entitled “The Effect of Design Patterns on (Present and Future) Cookie Consent Decisions” by Nataliia Bielova, Laura Litvine, Anysia Nguyen, Mariam Chammat, Vincent Toubiana and Estelle Hary.

Related publication: [20]

8.4 Research axis 4: Legal

8.4.1 The Conciliation Of Transparency Measures with the Processing of Possibly Sensitive Data by the Administration According to the French Administrative Judge

Participants: Alexandre Lodie.

The publication, on the French Ministry of Economy and Finance's website, of a Civil servant's appointment order whose legal basis lies on a decree concerning the access of disabled persons to state functions constitutes processing of data by automated means according to the Council of State. However, in judges' view, such processing cannot be seen as processing data "concerning health" pursuant to Article 9 of the GDPR. In this case, the plaintiff is a civil servant who has been appointed as Inspector of Finance according to a decree concerning the access of disabled persons to state functions. As provided by French Law, the appointment order – containing the legal basis of the nomination - was published on the Ministry of Economy and Finance's website. The claimant considered that the publication infringed his right to privacy and did not comply with the GDPR. In this decision, and contrary to what the Court of Appeal claimed, the Council of State concludes that the publication of the appointment order on the administration's website constitutes processing of data by automated means and is thus subject to the GDPR. However, since the appointment order does not reveal the nature of the disability, nor its seriousness, the Conseil d'Etat considers that it does not constitute processing of data concerning health. Such a decision seems to acknowledge a restrictive view of what constitutes "sensitive" data, which would not be in line with ECJ case law. Eventually, the Judges asked the administration to delete the mention of the decree in the appointment order as the appointment decision's period of appeal was over. Maintaining this information online was no longer necessary to achieve the purpose of the processing according to the French Administrative Judge.

Related publication: [5]

8.4.2 Are personal data always personal? Case T-557/20 SRB v. EDPS or when the qualification of data depends on who holds them

Participants: Alexandre Lodie.

In case T-557/20 Single Resolution Board v. EDPS, the General Court had to settle an issue related to the extent of the definition of 'personal data' under Article 3 (1) of Regulation 2018/1725 (hereafter 'EUDPR'). This case takes place in the context of the adoption of a resolution scheme, involving the Single Resolution Board (SRB), in its capacity of Banking Union resolution authority, and a Spanish bank called Banco Popular. During the process of resolution, the SRB invited the shareholders to submit comments in order to assess whether they should be given compensation. To examine these comments, the SRB classified them and attributed them an alphanumeric code. Some comments were sent to an independent valuer, Deloitte, to help complete the assessment. Following these events, five shareholders filed a complaint before the European Data Protection Supervisor (EDPS) on the ground that they had not been informed of their personal data being transferred to a third-party. Without digging into too much detail, the EDPS agreed with the complainants that their personal data had been processed by Deloitte while they had not been informed of any transfer of their data by the SRB. SRB, for its part, claimed that data processed by Deloitte were not personal data. Basically, the General Court had to determine whether the comments held by Deloitte could be considered personal data. To summarise the outcome of this case, the Court held that the transfer of comments which were attributed an alphanumeric code could not necessarily be considered as a transfer of personal data. Instead, it must be carefully assessed whether the data recipient is reasonably able to re-identify data subjects from the pseudonymised comments. The Court thus adopted a relative approach of what constitutes 'personal data' which, in our opinion, runs the risk of undermining the level of protection of personal data within the EU and the protection of personal data of EU citizens more globally.

Related publication: [22]

9 Bilateral contracts and grants with industry

9.1 Bilateral contracts with industry

OpenSezam

Participants: Mohamed Maouche, Vincent Roca.

- CIFRE PhD contract, 2024-2026 (website)
- The thesis is entitled: "Secure, Private and Multi-modal Authentication". The objective is to design an authentication system based on end-to-end machine learning, with an integrated system for continuous detection of anomalies and intrusions, using various types of biometric data, depending on the use-case.

10 Partnerships and cooperations

10.1 International initiatives

10.1.1 Associate Teams in the framework of an Inria International Lab or in the framework of an Inria International Program

MAGPIE: Machine Learning and privacy challenges

- Inria Associate Team, 2022-2024
- Partners: Inria PRIVATICS (coordinator), University College London (Emiliano De Cristofaro) (UK)
- Machine learning offers great potential but also comes with a number of drawbacks. In particular when ML is applied to personal data, the privacy of individual may be at risk. In an orthogonal approach, ML can be leveraged to tackle privacy issues, for instance by sanitizing data or automatically detecting issues in complex systems. In MAGPIE, two teams from UCL and Inria with a strong expertise in privacy and machine learning will collaborate to explore those two research directions.

10.1.2 Participation in other International Programs

Trusty AI: Enabling Privacy Preserving in Federated Learning

- Pack Ambition International / Face Foundation TJF, (2021-2023)
- Partners: Inria PRIVATICS (coordinator), University de Pennsylvanie
- Federated learning is a promising on-device machine learning scheme and new research topic on privacy-preserving machine learning. Federated learning becomes a paradigm shift in privacy-preserving AI and offers an attractive framework for training large-scale distributed learning models on sensitive data. However, federated learning still faces many challenges to fully preserve data privacy. This project tackles the cybersecurity challenges of federated learning systems in terms of data privacy. Specifically, the goal is to extend different federated learning approaches to consider their limitations in terms of accuracy, confidentiality, robustness, explainability and fairness.

10.2 International research visitors

10.2.1 Visits of international scientists

Inria International Chair

- Cristiana Santos, Inria International Chair (IIC Junior) laureate, Associate Professor at Utrecht University, join the team for 3 months per year, during the 2023-2026 period. She brings her legal expertise in EU Data Protection Laws to the PRIVATICS team.

Other international visits to the team

Colin M. Gray

Status Associate Professor

Institution of origin: Purdue University

Country: USA

Dates: 4 - 24 May 2023

Context of the visit: Collaboration on Dark Patterns Ontology

Mobility program/type of mobility: Visiting Researchers Program of the University Cote d'Azur

10.3 European initiatives

10.3.1 Other european programs/initiatives

PIVOT: Privacy-Integrated design and Validation in the constrained IoT

- ANR / BMBF French-German joint call on cybersecurity, 2021 - 2024.
- Partners: AFNIC (French coordinator), Freie Universität Berlin (German coordinator), Hamburg Univ. of Applied Science, Lobaro Industrial Solutions, INSA PRIVATICS
- The PIVOT project aims at assuring privacy of data and metadata with the low-end devices and low-power radio networks (e.g., LoRaWAN) of the ultra-constrained IoT, running the RIOT operating system. It focuses on: a cryptographic framework for privacy-friendly primitives, protocols that integrate decentralized object security, minimal trust anchor provisioning on IoT devices to enable object security, and multi-stakeholder name management that preserves privacy requirements and generates, allocates, and resolves names globally.

10.4 National initiatives

10.4.1 ANR

CISC

- Title: Certification of IoT Secure Compilation
- Type: ANR
- Duration: April 2018 - Sept. 2023
- Coordinator: Inria INDES project-team (France)
- Others partners: Inria CELTIC project-team (France), College de France (France)
- Abstract: The objective of the ANR CISC project is to investigate multitier languages and compilers to build secure IoT applications with private communication. A first goal is to extend multitier platforms by a new orchestration language that we call Hiphop.js to synchronize internal and external activities of IoT applications as a whole. CISC will define the language, semantics, attacker models, and policies for the IoT and investigate automatic implementation of privacy and security policies by multitier compilation of IoT applications. To guarantee such applications are correct, and in particular that the required security and privacy properties are achieved, the project will certify them using the Coq proof assistant.

PMR

- Title: Privacy-preserving methods for Medical Research
- Type: ANR
- Duration: 2020 - 2024
- Coordinator: Inria MAGNET
- Others partners: INSA Lyon, Creatis
- Abstract: Given the growing awareness of privacy risks of data processing, there is an increasing interest in privacy-preserving learning. However, shortcomings in the state of the art limit the applicability of the privacy-preserving learning paradigm. First, most approaches assume too optimistically a honest-but-curious setting. Second, most approaches consider one learning task in isolation, not accounting for the context where querying is a recurring activity. In this project, we will investigate new algorithms and models that address these shortcomings. Among others, (i) our algorithms will combine privacy-preserving properties of differential privacy with security offered by cryptography and (ii) based on models of information flows in integrated data handling processes, we will build more refined models analyzing the implications of repeated querying. We will demonstrate the utility of our new theory and algorithms by proposing strategies to realistically apply them in significant real-world problems illustrated through use cases in the medical domain.

PrivaWEB

- Title: Privacy Protection and ePrivacy Compliance for Web Users
- Type: ANR JCJC
- Duration: 2018 - 2023
- Coordinator: Inria - PRIVATICS
- Abstract: PrivaWEB aims at developing new methods for detection of advanced Web tracking technologies and new tools to integrate in existing Web applications that seamlessly protect privacy of users. In this project, we will integrate three key components into Web applications: privacy, compliance and usability. Our research will address methodological aspects (designing new detection methods and privacy protection mechanisms), practical aspects (large-scale measurement of Web applications, integration in existing Web browsers), and usability aspects (user surveys to evaluate privacy concerns and usability of existing and new protection tools).

IPoP

- Title: Interdisciplinary Project on Privacy
- Type: PEPR Cybersécurité / France 2030
- Duration: July 2022 - June 2028
- Coordinator: Inria - PRIVATICS
- Others partners: Inria COMET / MAGNET / PETRUS / MULTISPEECH and SPIRALS teams, CNRS - DCS lab., INSA CVL - LIFO lab., Univ. Grenoble Alps - CESICE lab., Univ. of Rennes 1 - SPICY team, EDHEC, CNIL
- Abstract: IPoP focuses on new forms of personal information collection, on AI models that preserve the confidentiality of personal information used, on data anonymization techniques, on securing personal data management systems, on differential privacy, on personal data legal protection and compliance, and all the associated societal and ethical considerations. This unifying interdisciplinary research program brings together recognized research teams (universities, engineering schools and institutions) and the CNIL.

SSF-ML-DH

- Title: Secure, safe and fair machine learning for healthcare
- Type: PEPR Santé Numérique / France 2030
- Duration: November 2023 - October 2027
- Coordinator: Inria - MAGNET
- Others partners: Inria PRIVATICS, Inria EPIONE, CNRS Lamsade, Cea - List, IMT Atlantique, CNRS Diens
- Abstract: The healthcare sector generates vast amounts of data from various sources (e.g., electronic health records, imaging, wearable devices, or population health data). These datasets, analyzed through ML systems, could improve the whole healthcare system, for the individuals and the society. However, the sensitive nature of health data, cybersecurity risks, biases in the data, and the lack of robustness of ML algorithms are all factors that currently limit the widespread use of such data bases. The project aims to develop new ML algorithms, designed to handle the unique characteristics of multi-scale and heterogeneous individual health data, while providing formal privacy guarantees, robustness against adversarial attacks and changes in data dynamics, and fairness for under-represented populations.

10.4.2 INRIA-CNIL collaboration

PRIVATICS and CNIL collaborate since 2012 through several collaborative projects (e.g., the Mobilitics bi-lateral project on privacy and smartphones in 2012-2014, the IoTics ANR research project on privacy and connected devices), workshops and discussions on data anoymisation, risk analysis, consent or IoT Privacy. PRIVATICS is also in charged of the organization of the CNIL-Inria prize that is awarded every year to an outstanding publication in the field of data privacy.

Last but not least:

- Nataliia Bielova worked in the Laboratoire d'Innovation de la CNIL (LINC) in the context of a "mise à disposition", from September 2021 to December 2022. News CNIL
- On August 2021, Claude Castelluccia was appointed member of the CNIL Board ("commissaire CNIL") as one qualified public figures for his expertise on digital sciences and privacy questions. As such he is in charge of several domains and contributes to the doctrine of the French Data Protection Authority. This is a *major involvement representing approximately 80% of his professional activity*.

10.4.3 Inria Exploratory Action (AEx)

DATA4US (Personal DAta TrAnsparency for web USers)

- Participants: Cedric Lauradoux, Nataliia Bielova
- Duration: 2020-2024
- Abstract: Since May 2018, General Data Protection Regulation (GDPR) regulates collection of personal data in all EU countries, but users today are still tracked and their data is still silently collected as they browse the Web. GDPR empowers users with the rights to access their own data, but users have no means to exercise their rights in practice. DATA4US tackles these interdisciplinary challenges by establishing collaborations with researchers in Law. DATA4US will propose a new architecture for exercising access rights that will explain the users whether their data has been legally collected and eventually help contact DPAs for further investigations.

10.4.4 Inria Action de Dévelopement Technologique (ADT)

PRESERVE (Plate-foRme wEb de SEnsibilisation aux pRoblèmes de Vie privéE):

- Participant: Antoine Boutet, Adrien Baud.
- Abstract: The goal of the PRESERVE ADT is to design a platform whose goal is to raise users' awareness of privacy issues. The first version implements tools in order to inspect location history. Specifically, this version implements [hal-02421828] where a user is able to inspect the private and sensitive information inferred from its own location data.

11 Dissemination

11.1 Promoting scientific activities

11.1.1 Scientific events: organisation

General chair, scientific chair

- Cédric Lauradoux: *General Chair* of the Annual Privacy Forum 2023, Lyon, May 2023.

Member of the organizing committees

- Antoine Boutet co-organized the GDR RSD / ASF Winter School on Distributed Systems and Networks from 2019 to 2023.
- Antoine Boutet: co-organizer of the summer school and the days on decentralized learning, 2023
- Antoine Boutet: co-organizer of the ASF Winter School on Distributed Systems and Networks 2020-2024, Sept Laux, France.
- Nataliia Bielova: Organizer and moderator of the panel on *Dark Patterns: definitiona dn evidence for regulators*, at CPDP conference, Brussels, May 2023.

11.1.2 Scientific events: selection

Chair of conference program committees

- Nataliia Bielova: *vice-PC Chair* of the USENIX Security Symposium 2023.
- Nataliia Bielova: *co-Chair* of the CNIL-Inria Privacy Protection Award.

Member of the conference program committees

- Mathieu Cunche: member of TPC for ACM AsiaCCS 2023
- Mathieu Cunche: member of TPC for ACM WiSec 2023
- Mathieu Cunche: member of TPC for DPM 2023
- Antoine Boutet: member of TPC for SRDS 2023
- Nataliia Bielova: member of TPC for ConPro 2023
- Nataliia Bielova: member of TPC for MADWeb 2023

11.1.3 Invited talks

- Antoine Boutet: organizer and moderator of the panel "Processing Health Data: Challenges and Way Forward" at APF conference, June 2023.
- Antoine Boutet: organizer and moderator of the panel "Problématique de l'apprentissage fédéré en santé", at the summer school on decentralized learning, September 2023.
- Antoine Boutet: participant of the panel "Les données synthétiques : encadrement et enjeux des techniques et des usages", at the ekitia seminar, November 2023.
- Nataliia Bielova: invited talk on online tracking and consent at EPFL SPRING lab, Lausanne, Switzerland.
- Nataliia Bielova: invited talk at UK Cyber Security and Privacy Seminar Series on technical and legal perspectives of Web Privacy, online event.
- Nataliia Bielova: invited talk at Harvard Law School's Beyond the FTC event, the first symposium at Harvard on Privacy for Legal and Computer Scientists, Harvard Law School, Cambridge, USA.
- Nataliia Bielova: keynote speaker at the Annual Conference of the French Association of Law and Economics (AFED), Nice, October 2023.
- Nataliia Bielova and Claude Castelluccia: invited speakers at the 2nd workshop of the event series Vers un droit neuro-éthique, Paris, November 2023.

11.1.4 Leadership within the scientific community

- Mathieu Cunche, co-chair of the Privacy Protection (PVP) Working Group of *GDR Sécurité*
- Nataliia Bielova: member of steering committee for Atelier sur la Protection de la Vie Privée (French workshop on Privacy Protection), 2022-ongoing.
- Antoine Boutet, chair of the Privacy Protection Working Group of the French-Japan Cybersecurity Collaboration

11.2 Teaching - Supervision - Juries

11.2.1 Teaching

Most of the PRIVATICS members' lectures are given at INSA-Lyon (Antoine Boutet and Mathieu Cunche are associated professor at INSA-Lyon), at Grenoble Alps University (Claude Castelluccia, Vincent Roca and Cédric Lauradoux), and Université Côte d'Azur (Nataliia Bielova).

Most of the PRIVATICS members' lectures are on the foundations of computer science, security and privacy, as well as networking. The lectures are given to computer science students but also to business school students and to laws students.

Details of lectures:

- Master : Antoine Boutet, *Privacy*, 80h, INSA-Lyon, France.
- Master : Antoine Boutet, *Security*, 40h, INSA-Lyon, France.
- Undergraduate course : Mathieu Cunche, *Introduction to computer science*, 120h, L1, INSA-Lyon, France.
- Master : Mathieu Cunche, *Wireless Security*, 6h, M2, INSA-Lyon, France.
- Undergraduate course : Mathieu Cunche, *On Wireless Network Security*, 10h, L1, IUT-2 (UPMF - Grenoble University) , France.
- Undergraduate course : Mathieu Cunche, *Systems and Networks Security* , 10h, M2, INSA-Lyon, France.

- Master : Mathieu Cunche, *Privacy and Data protection*, 26h, M2, INSA-Lyon, France.
- Master : Mathieu Cunche, *Cryptography and Communication Security*, 18h, M1, INSA-Lyon, France.
- Master : Cédric Lauradoux, *Advanced Topics in Security*, 20h, M2, Ensimag/INPG, France.
- Master : Cédric Lauradoux, *Systems and Network Security*, 30h, M1, Ensimag, France.
- Master : Cédric Lauradoux, *Internet Security*, 12h, M2, University of Grenoble Alpes, France.
- Master : Cédric Lauradoux, *Cyber Security*, 3h, M2, Laws School of University of Grenoble Alpes, France.
- Master : Claude Castelluccia, *Advanced Topics in Security*, 15h, M2, Ensimag/INPG, France.
- Master : Claude Castelluccia, *Cyber Security*, 6h, M2, Laws School of University of Grenoble Alpes, France.
- Master : Claude Castelluccia, *Data Privacy*, 6h, M2, Laws School of University of Grenoble Alpes, France.
- Master : Claude Castelluccia, *Data Privacy*, 12h, SKEMA Business School, Sophia-Antipolis, France.
- Master : Vincent Roca, *Wireless Communications*, 16h, M2, Polytech, University of Grenoble Alpes, France.
- Undergraduate course : Vincent Roca, *C Programming and Security*, 24h, L-Pro, IUT-2 (University of Grenoble Alpes), France.
- Undergraduate course : Vincent Roca, *Privacy in Smartphones and Internet of Things*, 3h, L-Pro, University of Grenoble Alpes, France.
- Master : Vincent Roca, *Privacy in Smartphones and Internet of Things*, 3h, M2, Ensimag/INPG, France.
- Master : Vincent Roca, *Privacy in Smartphones*, 1.5h, M2 (University of Cote-d'Azur), France.

11.2.2 Supervision

PhD defended in 2023:

- Michael Toth, *"Consent on the Web: a transdisciplinary analysis"*, co-supervised by Nataliia Bielova and Vincent Roca, Doctoral School of University of Nice, defended on June 19th, 2023.
- Coline Boniface, *"The attribution of cyber attacks: a sovereign state power?"*, Law Doctoral School of University Grenoble Alpes (UGA), co-supervised by Cédric Lauradoux and Karine Bannelier, defended on December 12th, 2023.

On-going PhDs:

- Samuel Pelissier, co-supervised by Mathieu Cunche and Vincent Roca
- Jan Aalmoes, co-supervised by Antoine Boutet, Carole Frindel and Mathieu Cunche
- Thomas Lebrun, co-supervised by Antoine Boutet, Claude Castellucccia and Mathieu Cunche
- Gilles Mertens, *"Progressive Web Apps"*, co-supervised by Vincent Roca, Mathieu Cunche and Nataliia Bielova
- Teodora Curelariu, *"Cyber-incidents entre monde privé et public"*, co-supervised by Cédric Lauradoux and Karine Bannelier

New PhD:

- Alix Ntoutoume, CIFRE PhD with the OpenSezam company, co-supervised by Mohamed Maouche, Vincent Roca, and Pierre-Guillaume Gourio-Jewell, since Dec. 2023

Stopped PhD:

- Suzanne Lansade, PhD stoppped for personal reasons

11.2.3 Juries

Vincent Roca took part to several PhD juries:

- **Examiner** of the PhD thesis of M. Matthieu Petrou, "Collection de données et analyse de la qualité d'expérience utilisateur des systèmes de communication par satellite", Université de Toulouse, December 2023.
- **Reviewer** of the PhD thesis of M. Nathanaël Denis, "For a Private and Secure Internet of Things with Usage Control and Distributed Ledger Technology", Thèse de doctorat de l'Institut Polytechnique de Paris, October 2023.
- **Reviewer** of the PhD thesis of M. Paul Olivier, "Improving Hardware-in-the-loop Dynamic Security Testing For Linux-based Embedded Devices", Sorbonne Université. tel-04112035, March 2023.

Mathieu Cunche took part to the following PhD jury :

- **Examiner** of the PhD thesis of M. Abhishek Kumar Mishra, "Revealing and exploiting privacy vulnerabilities in users' public wireless packets", Institut polytechnique de Paris, October 2023.

Antoine Boutet took part to the following PhD juries:

- **Examiner** of the PhD thesis of M. Carlos Antonio Pinzón Henao, "Exploring Fairness and Privacy in Machine Learning", Thèse de doctorat de l'Institut Polytechnique de Paris, December 2023.
- **Examiner** of the PhD thesis of M. Yakini Tchouka, "Dé-identification des comptes rendus médicaux pour les tâches d'apprentissage automatique : application à l'association des codes CIM-10", Thèse de doctorat de l'Université Bourgogne-France-Comté, December 2023.

Claude Castelluccia took part to the following Habilitation jury:

- **Reviewer and President** of the Habilitation thesis of M. Francois Viangalli, "Le Concept de donnée", Thèse d'habilitation de l'Université Grenoble Alpes, December 2023.

Nataliia Bielova took part in the following PhD juries:

- **Reviewer** of the Phd thesis of Karel Kubicek, "Automated Analysis and Enforcement of Consent Compliance", ETH Zurich (Switzerland), December 2023.
- **Reviewer** of the PhD thesis of Romain Fouquet, "Préserver la vie privée en ligne grâce au blocage de contenu", University of Lille (France), May 2023.

11.3 Popularization

11.3.1 Articles and contents

- **Le Journal du Dimanche**, Comment votre téléphone vous espionne, Mathieu Cunche, 02/03/23
- **Sciences et Avenir**, Le rêve d'un Internet sans mot de passe, Mathieu Cunche, 01/03/23
- **The Conversation:** Données personnelles : rien à cacher, mais beaucoup à perdre, Antoine Boutet, 29/03/2023
- **The Conversation:** ChatGPT, modèles de langage et données personnelles : quels risques pour nos vies privées ?, Antoine Boutet, 23/06/2023

11.3.2 Interventions

- Vincent Roca gave two conferences for the "Université Inter-Age du Dauphiné", Respect de la vie privée et protection des données à caractère personnel, January and May 2023.
- Mathieu Cunche gave a conference at INSA-Lyon, "Sommes-nous écoutés par les objets de notre vie quotidienne ?", December 2023

12 Scientific production

12.1 Major publications

[1] C. Cholez, I. Joly, S. Astor, M. Steffen, V. Roca, S. Mika and H. Bean. *COVoM : Covid On My Mobile: To what extent Contact-Tracing Apps become a tool in policymakers' and citizens' hands?* University of Grenoble-Alpes, 20th Sept. 2023, pp. 1–22. URL: https://shs.hal.science/halshs-04219431.

[2] G. Gagnon, S. Gambs and M. Cunche. 'RSSI-based Fingerprinting of Bluetooth Low Energy Devices'. In: SECRYPT 2023 - 20th International Conference on Security and Cryptography. Rome, Italy, 10th July 2023, pp. 1–12. URL: https://inria.hal.science/hal-04161424.

[3] A. Lodie. 'The Conciliation Of Transparency Measures with the Processing of Possibly Sensitive Data by the Administration According to the French Administrative Judge'. In: *European Review of Digital Administration & Law* 3.2 (2023), pp. 233–239. DOI: 10.53136/979122180798120. URL: https://hal.science/hal-04299614.

[4] T. Pascoal, J. Decouchant, A. Boutet and M. Völp. 'I-GWAS: Privacy-Preserving Interdependent Genome-Wide Association Studies'. In: PETS 2023 - 23rd Privacy Enhancing Technologies Symposium. Lausanne, Switzerland, 10th July 2023. URL: https://hal.inria.fr/hal-03781755.

12.2 Publications of the year

International journals

[5] A. Lodie. 'The Conciliation Of Transparency Measures with the Processing of Possibly Sensitive Data by the Administration According to the French Administrative Judge'. In: *European Review of Digital Administration & Law* 3.2 (2023), pp. 233–239. DOI: 10.53136/979122180798120. URL: https://hal.science/hal-04299614.

Invited conferences

[6] A. Boutet and I. Sandu Popa. 'Tutorial: Trusted Execution Environments and Intel SGX - a few basic notions and usages'. In: RESSI 2023 - Rendez-vous de la Recherche et de l'Enseignement de la Sécurité des Systèmes d'Information. Neuvy-sur-Barangeon, France, 2023. URL: https://inria.hal.science/hal-04228113.

International peer-reviewed conferences

[7] G. Berthelier, A. Boutet and A. Richard. 'Toward training NLP models to take into account privacy leakages'. In: BigData 2023 - IEEE International Conference on Big Data. Sorrento, Italy: IEEE, 2023, pp. 1–9. URL: https://hal.science/hal-04299405.

[8] A. Boutet, C. Frindel and M. Maouche. 'Towards an evolution in the characterization of the risk of re-identification of medical images'. In: BigData 2023 - IEEE International Conference on Big Data. Sorrento, Italy: IEEE, 2023, pp. 1–6. URL: https://hal.science/hal-04299422.

[9] G. Gagnon, S. Gambs and M. Cunche. 'RSSI-based Fingerprinting of Bluetooth Low Energy Devices'. In: SECRYPT 2023 - 20th International Conference on Security and Cryptography. Rome, Italy, 10th July 2023, pp. 1–12. URL: https://inria.hal.science/hal-04161424.

[10] F.-X. Molina, V. Roca, R. Dagher, E. Baccelli, N. Mitton, A. Boutet and M. Cunche. 'PEPPER: Precise Privacy-Preserving Contact Tracing with Cheap, BLE/UWB Capable Tokens'. In: WoWMoM 2023 - 24th IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks. Boston, United States: IEEE, 12th June 2023, pp. 1–10. URL: https://inria.hal.science/hal-04064415.

[11] D. Nurbakova, A. Serna, A. Omiri and A. Boutet. 'Adaptive and Privacy-Aware Persuasive Strategies to Promote Healthy Eating Habits: Position Paper'. In: UMAP 2023 - 31st ACM Conference on User Modeling, Adaptation and Personalization. UMAP '23 Adjunct: Adjunct Proceedings of the 31st ACM Conference on User Modeling, Adaptation and Personalization. Limassol, Cyprus: ACM, 2023, pp. 129–131. DOI: 10.1145/3563359.3596987. URL: https://hal.science/hal-04142017.

[12] T. Pascoal, J. Decouchant, A. Boutet and M. Völp. 'I-GWAS: Privacy-Preserving Interdependent Genome-Wide Association Studies'. In: PETS 2023 - 23rd Privacy Enhancing Technologies Symposium. Lausanne, Switzerland, 10th July 2023, pp. 1–17. URL: https://inria.hal.science/hal-03781755.

National peer-reviewed Conferences

[13] G. Berthelier, A. Boutet and A. Richard. 'Privacy leakages on NLP models and mitigations through a use case on medical data'. In: COMPAS 2023 - Conférence francophone d'informatique en Parallélisme, Architecture et Système. Annecy, France, 2023, pp. 1–8. URL: https://inria.hal.science/hal-04138528.

Conferences without proceedings

[14] A. Boutet and V. Roca. 'IPoP: Interdisciplinary Project on Privacy'. In: RESSI 2023 - Rendez-vous de la Recherche et de l'Enseignement de la Sécurité des Systèmes d'Information. Neuvy-sur-Barangeon, France, 2023. URL: https://inria.hal.science/hal-04233354.

[15] C. Cholez and V. Roca. 'The throes of measuring the effectiveness of a public policy digital solution. Looking for contact tracing apps' users in covid19 time'. In: 2023 - 6th Nordic STS Conference. Oslo, Norvège, Norway, 2023. URL: https://shs.hal.science/halshs-04207595.

Doctoral dissertations and habilitation theses

[16] M. Toth. 'Consent on the web : a transdisciplinary analysis'. Université Côte d'Azur, 19th June 2023. URL: https://theses.hal.science/tel-04259483.

Reports & preprints

[17] L. Bart, E. A. Bechorfa, A. Boutet, J. Ramon and C. Frindel. *A Smartphone-based Architecture for Prolonged Monitoring of Gait*. Insa Lyon; Inria Lyon, 20th Dec. 2023. URL: https://hal.science/hal-04355370.

[18] C. Cholez, I. Joly, S. Astor, M. Steffen, V. Roca, S. Mika and H. Bean. *COVoM : Covid On My Mobile: To what extent Contact-Tracing Apps become a tool in policymakers' and citizens' hands?* University of Grenoble-Alpes, 20th Sept. 2023, pp. 1–22. URL: https://shs.hal.science/halshs-04219431.

[19] K. Makhlouf, H. H. Arcolezi, S. Zhioua, G. B. Brahim and C. Palamidessi. *On the Impact of Multi-dimensional Local Differential Privacy on Fairness*. 7th Dec. 2023. URL: https://hal.science/hal-04329938.

Other scientific publications

[20] N. Bielova, M. Chammat, V. Toubiana, E. Hary, A. Nguyen and L. Litvine. *The Effect of Design Patterns on (Present and Future) Cookie Consent Decisions: Supplemental Materials*. Philadelphia, United States, 14th Aug. 2024. URL: https://inria.hal.science/hal-04235032.

[21] J. Detchart, E. Lochin, J. Lacan and V. Roca. *RFC 9407 Tetrys: An On-the-Fly Network Coding Protocol.* 12th June 2023. URL: https://hal.science/hal-04126816.

[22] A. Lodie. *Are personal data always personal? Case T-557/20 SRB v. EDPS or when the qualification of data depends on who holds them.* 7th Nov. 2023. URL: https://hal.science/hal-04292464.

12.3 Other

Scientific popularization

[23] G. Berthelier and A. Boutet. *ChatGPT, modèles de langage et données personnelles : quels risques pour nos vies privées ?* 23rd June 2023. URL: https://hal.science/hal-04371691.

[24] A. Boutet. *Données personnelles : rien à cacher, mais beaucoup à perdre.* 29th Mar. 2023. URL: https://hal.science/hal-04316957.