RESEARCH CENTRES

Inria Center
at Université Grenoble Alpes

Inria Lyon Center

2022
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

A1.2.8. – Network security

A1.3.1. – Web

A4.8. – Privacy-enhancing technologies

A9.2. – Machine learning

A9.9. – Distributed AI, Multi-agent

Other research topics and application domains

B6. – IT and telecom

B6.2.2. – Radio technology

B6.3.1. – Web

B6.3.2. – Network protocols

B6.3.4. – Social Networks

B6.4. – Internet of things

B6.6. – Embedded systems

B7.2. – Smart travel

B7.2.1. – Smart vehicles

B7.2.2. – Smart road

B8.1.2. – Sensor networks for smart buildings

B8.2. – Connected city

B9.1.1. – E-learning, MOOC

B9.5.6. – Data science

B9.6.2. – Juridical science

B9.6.5. – Sociology

B9.9. – Ethics

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]
- Cedric Lauradoux [INRIA, Researcher]
- Mohamed Maouche [INRIA, Researcher]

Faculty Members

- Antoine Boutet [INSA LYON, Associate Professor]
- Mathieu Cunche [INSA LYON, Associate Professor, HDR]

PhD Students

- Jan Aalmoes [INSA LYON]
- Coline Boniface [UGA, École doctorale Sciences Juridiques (EDSJ) de l'UGA]
- Teodora Curelariu [UGA, from Dec 2022, École doctorale Sciences Juridiques (EDSJ) de l'UGA]
- Suzanne Lansade [INRIA]
- Thomas Lebrun [INRIA]
- Gilles Mertens [INRIA, from Nov 2022]
- Samuel Pelissier [INSA LYON]
- Michael Toth [INRIA]

Technical Staff

- Julien Barnier [CNRS, Engineer, from Nov 2022]
- Adrien Baud [INRIA, Engineer, from Feb 2022]
- Amine Mohamed Berchorfa [INSA LYON, Engineer, from Nov 2022, accueil au laboratoire INSERM / CREATIS]

Interns and Apprentices

- Mohamed Bechorfa [INSA LYON, from Apr 2022]
- Amine Mohamed Berchorfa [INSA LYON, Intern, from Apr 2022 until Aug 2022, accueil au laboratoire INSERM / CREATIS]
- Javiera Bermudez Alegria [INRIA, from Mar 2022 until Jun 2022, INRIA-Chile exchange program]
- Teodora Curelariu [UGA, from Jun 2022 until Aug 2022]
- Gilles Mertens [INRIA, from Mar 2022 until Sep 2022]
- Thi Mai Phuong Nguyen [INRIA, from Mar 2022 until Aug 2022]
- Jingyao Wang [INSA LYON, Intern, from Mar 2022 until Aug 2022]

Administrative Assistant

- Helen Pouchot-Rouge-Blanc [INRIA]

2 Overall objectives

2.1 Context

Since its creation in 2014, the PRIVATICS project-team focusses on privacy protection in the digital world. It includes, on one side, activities that aim at understanding the domain and its evolution, both from theoretical and practical aspects, and, on the other side, activities that aim at designing privacy-enhancing tools and systems. The approach taken in PRIVATICS is fundamentally inter-disciplinary and covers theoretical, legal, economical, sociological and ethical aspects by the means of enriched collaborations with the members of these disciplines.

3 Research program

Privacy is essential to protect individuals, but also to protect the society, for instance to avoid the misuse of personal data to surreptitiously manipulate individuals in elections. In this context, the PRIVATICS team carries out a broad range of research activities: some of them aim at understanding the domain and its evolution, both from the theoretical and practical viewpoints, while others aim at designing privacy-enhancing tools and systems.

Examples of the PRIVATICS team research activities, always with privacy as a common denominator, include:

- federated machine learning;
- explainability of automatic decision making systems;
- user manipulation through dark patterns;
- identification and protection against web tracking;
- privacy leaks in IoT, smartphone applications and wireless networks;
- PDF document sanitization; privacy in digital health tools;
- digital contact tracing in the TousAntiCovid system;
- legal considerations in privacy;
- societal considerations, for instance in the context of video-surveillance systems;
- and theoretical foundations for privacy, for instance with formal languages for privacy policies.

The domain of privacy and personal data protection is clearly fundamentally multifacted, from scientific and technical aspects to legal, economic, sociological, ethic and cultural aspects. Whenever it makes sense, PRIVATICS will continue to favor interdisciplinarity, through collaborations with colleagues from other disciplines.

4 Application domains

4.1 Domain 1: Privacy in smart environments

One illustrative example is our past work on privacy-preserving smart-metering [2]. Several countries throughout the world are planning to deploy smart meters in house-holds in the very near future. Traditional electrical meters only measure total consumption on a given period of time (i.e., one month or one year). As such, they do not provide accurate information of when the energy was consumed. Smart meters, instead, monitor and report consumption in intervals of few minutes. They allow the utility provider to monitor, almost in real-time, consumption and possibly adjust generation and prices according to the demand. Billing customers by how much is consumed and at what time of day will probably change consumption habits to help matching energy consumption with production. In the longer term, with the advent of smart appliances, it is expected that the smart grid will remotely control selected appliances to reduce demand. Although smart metering might help improving energy management, it creates many new privacy problems. Smart-meters provide very accurate consumption data to electricity providers. As the interval of data collected by smart meters decreases, the ability to disaggregate low-resolution data increases. Analysing high-resolution consumption data, Non-intrusive Appliance Load Monitoring (NALM) can be used to identify a remarkable number of electric appliances (e.g., water heaters, well pumps, furnace blowers, refrigerators, and air conditioners) employing exhaustive appliance signature libraries. We developed DREAM, DiffeRentially privatE smArt Metering, a scheme that is private under the differential privacy model and therefore provides strong and provable guarantees. With our scheme, an (electricity) supplier can periodically collect data from smart-meters and derive aggregated statistics while learning only limited information about the activities of individual households. For example, a supplier cannot tell from a user's trace when he watched TV or turned on heating.

4.2 Domain 2: Big Data and Privacy

We believe that another important problem will be related to privacy issues in big data. Public datasets are used in a variety of applications spanning from genome and web usage analysis to location-based and recommendation systems. Publishing such datasets is important since they can help us analyzing and understanding interesting patterns. For example, mobility trajectories have become widely collected in recent years and have opened the possibility to improve our understanding of large-scale social networks by investigating how people exchange information, interact, and develop social interactions. With billions of handsets in use worldwide, the quantity of mobility data is gigantic. When aggregated, they can help understand complex processes, such as the spread of viruses, and build better transportation systems. While the benefits provided by these datasets are indisputable, they unfortunately pose a considerable threat to individual privacy. In fact, mobility trajectories might be used by a malicious attacker to discover potential sensitive information about a user, such as his habits, religion or relationships. Because privacy is so important to people, companies and researchers are reluctant to publish datasets by fear of being held responsible for potential privacy breaches. As a result, only very few of them are actually released and available. This limits our ability to analyze such data to derive information that could benefit the general public. It is now an urgent need to develop Privacy-Preserving Data Analytics (PPDA) systems that collect and transform raw data into a version that is immunized against privacy attacks but that still preserves useful information for data analysis. This is one of the objectives of Privatics. There exists two classes of PPDA according to whether the entity that is collecting and anonymizing the data is trusted or not. In the trusted model, that we refer to as Privacy-Preserving Data Publishing (PPDP), individuals trust the publisher to which they disclose their data. In the untrusted model, that we refer to as Privacy-Preserving Data Collection (PPDC), individuals do not trust the data publisher. They may add some noise to their data to protect sensitive information from the data publisher.

Privacy-Preserving Data Publishing: In the trusted model, individuals trust the data publisher and disclose all their data to it. For example, in a medical scenario, patients give their true information to hospitals to receive proper treatment. It is then the responsibility of the data publisher to protect privacy of the individuals' personal data. To prevent potential data leakage, datasets must be sanitized before possible release. Several proposals have been recently proposed to release private data under the Differential Privacy model [25, 56, 26, 57, 50]. However most of these schemes release a "snapshot" of the datasets at a given period of time. This release often consists of histograms. They can, for example, show the distributions of some pathologies (such as cancer, flu, HIV, hepatitis, etc.) in a given population. For many analytics applications, "snapshots" of data are not enough, and sequential data are required. Furthermore, current work focusses on rather simple data structures, such as numerical data. Release of more complex data, such as graphs, are often also very useful. For example, recommendation systems need the sequences of visited websites or bought items. They also need to analyse people connection graphs to identify the best products to recommend. Network trace analytics also rely on sequences of events to detect anomalies or intrusions. Similarly, traffic analytics applications typically need sequences of visited places of each user. In fact, it is often essential for these applications to know that user A moved from position 1 to position 2, or at least to learn the probability of a move from position 1 to position 2. Histograms would typically represent the number of users in position 1 and position 2, but would not provide the number of users that moved from position 1 to position 2. Due to the inherent sequentiality and high-dimensionality of sequential data, one major challenge of applying current data sanitization solutions on sequential data comes from the uniqueness of sequences (e.g., very few sequences are identical). This fact makes existing techniques result in poor utility. Schemes to privately release data with complex data structures, such as sequential, relational and graph data, are required. This is one the goals of Privatics. In our current work, we address this challenge by employing a variable-length n-gram model, which extracts the essential information of a sequential database in terms of a set of variable-length n - grams [15]. We then intend to extend this approach to more complex data structures.

Privacy-Preserving Data Collection: In the untrusted model, individuals do not trust their data publisher. For example, websites commonly use third party web analytics services, such as Google Analytics to obtain aggregate traffic statistics such as most visited pages, visitors' countries, etc. Similarly, other applications, such as smart metering or targeted advertising applications, are also tracking users in order to derive aggregated information about a particular class of users. Unfortunately, to obtain this aggregate information, services need to track users, resulting in a violation of user privacy. One of our goals is to develop Privacy-Preserving Data Collection solutions. We propose to study whether it is possible to provide efficient collection/aggregation solutions without tracking users, i.e. without getting or learning individual contributions.

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 sometimes leads us to promote local data 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

Several of PRIVATICS works had major societal impacts. One can cite:

- The ROBERT Exposure Notification Protocol and the CLEA Cluster Exposure Verification Protocol, both of them being at the core of the StopCovid/TousAntiCovid application (see our ROBERT/DESIRE website);
- The work on tracking technologies and the use of consent banners in web browsers (e.g., [6]). This work helped revealing practices in the field, sometimes highlighting illegal practices, and therefore it helped promoting a more privacy friendly society;
- The popular "Protection de la vie privée dans le monde numérique" Massive Online Course (MOOC) on the FUN platform;

Additionally, several PRIVATICS members are part of several 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 Recrutment of Mohamed Maouche as permanent researcher

Mohamed joined the PRIVATICS research team on December 2022, as permanent researcher (ISFP). After a PhD in computer science from INSA-Lyon on the topic of location privacy, he joined the Magnet team and focussed on private machine learning for speech processing, and more recently in the DSVD Chaire in partnership with Renault Group on personal data collection in vehicular safety systems.

His main interest is to build machine learning systems that manage a good trade-off between privacy and utility. He also explores anonymization techniques and re-identification threats on different data types and applications.

6.2 Awards: Best thesis prize from INSA-Lyon for Clément Henin

Clément Henin received the **Best thesis prize from INSA-Lyon**. He defended his PhD on October 2021, under the supervision of by Daniel Le Métayer and Claude Castelluccia, thesis entitled:
"Explanations and justifications of algorithmic decisions"
The ceremony took place on Nov. 2022, Campus de la Doua, Villeurbanne.

6.3 IPoP Project on Privacy - Cybersecurity PEPR

Official launch of the Interdisciplinary Project on Privacy (IPoP), in the context of the CyberSecurity PEPR (France 2030). This project is leaded by PRIVATICS (Antoine Boutet and Vincent Roca)

The project's scientific program focuses on new forms of personal information collection, on the learning of Artificial Intelligence (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 internationally recognized research teams (from universities, engineering schools and institutions) working on privacy, and the French Data Protection Authority (CNIL).

IPoP web site

6.4 Impact of our research on policy makers and regulators

Natalia Bielova has established a collaboration with researcher in design Colin M. Gray and a researcher in law Cristiana Santos. This collaboration has led to a remarkably new and influential paper on dark patterns and legal requirements of cookie banners, published in 2021. This work has been cited in the following reports by regulators in 2022:

- OECD report on Dark commercial patterns
- European Commission study on unfair commercial practices in the digital environment
- UK Competition and Markets Authorithy report on Online Choice Architecture

Vincent Roca, Nataliia Bielova, Michael Toth and external collaborators Cristiana Santos and Midas Nouwens analyzed the practices of the consent banner providers, investigating legal roles and responsibilities of each actor. Thanks to the arguments in the APF 2021 paper, these companies have been then reclassified as "data controllers", rather than mere processors. This work had an immediate practical importance:

- Belgian Data Protection Authority used arguments presented in the paper in its sanction decision to fine IAB Europe over its consent framework's GDPR violations.

7 New software and platforms

7.1 New software

7.2 New platforms

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

Participants: Antoine Boutet, Adrien Baud.

This platform aims to raise users' awareness of privacy issues. It aims to be used as a front for several works of the Privatics team as well as for collaborations and actions. 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. This platform will be enriched with new functionalities in the future.

8 New results

8.1 On the topic of privacy considerations in websites, wireless networks and Internet of Things

8.1.1 On dark patterns and manipulation of website publishers by CMPs

Participants: Michael Toth, Nataliia Bielova, Vincent Roca.

Web technologies and services widely rely on data collection via tracking users on websites. In the EU, the collection of such data requires user consent thanks to the ePrivacy Directive (ePD), and the General Data Protection Regulation (GDPR). To comply with these regulations and integrate consent collection into their websites, website publishers often rely on third-party contractors, called Consent Management Providers (CMPs), that provide consent pop-ups as a service. Since the GDPR came in force in May 2018, the presence of CMPs continuously increased. In our work, we systematically study the installation and configuration process of consent pop-ups and their potential effects on the decision making of the website publishers. We make an in-depth analysis of the configuration process from ten services provided by five popular CMP companies and identify common unethical design choices employed. By analysing CMP services on an empty experimental website, we identify manipulation of website publishers towards subscription to the CMPs paid plans and then determine that default consent pop-ups often violate the law. We also show that configuration options may lead to non-compliance, while tracking scanners offered by CMPs manipulate publishers. Our findings demonstrate the importance of CMPs and design space offered to website publishers, and we raise concerns around the privileged position of CMPs and their strategies influencing website publishers.

Related publication: [6]

8.1.2 My Cookie is a phoenix: detection, measurement, and lawfulness of cookie respawning with browser fingerprinting

Participants: Imane Fouad, Cristiana Santos, Arnaud Legout, Nataliia Bielova.

Stateful and stateless web tracking gathered much attention in the last decade, however they were always measured separately. To the best of our knowledge, our study is the first to detect and measure cookie respawning with browser and machine fingerprinting. We develop a detection methodology that allows us to detect cookies dependency on browser and machine features. Our results show that 1,150 out of the top 30,000 Alexa websites deploy this tracking mechanism. We find out that this technique can be used to track users across websites even when third-party cookies are deprecated. Together with a legal scholar, we conclude that cookie respawning with browser fingerprinting lacks legal interpretation under the GDPR and the ePrivacy directive, but its use in practice may breach them, thus subjecting it to fines up to 20 million Euros.

Related publication: [2]

8.1.3 Device re-identification in LoRaWAN through messages linkage

Participants: Samuel Pelissier, Mathieu Cunche, Vincent Roca.

In LoRaWAN networks, devices are identified by two identifiers: a globally unique and stable one called DevEUI, and an ephemeral and randomly assigned pseudonym called DevAddr. The association between those identifiers is only known by the network and join servers, and is not available to a passive eavesdropper. In this work, we consider the problem of linking the DevAddr with the corresponding DevEUI based on passive observation of the LoRa traffic transmitted over the air. Leveraging metadata exposed in LoRa frames, we devise a technique to link two messages containing respectively the DevEUI and the DevAddr, thus identifying the link between those identifiers. The approach is based on machine learning algorithms using various pieces of information including timing, signal strength, and fields of the frames. Based on an evaluation using a real-world dataset of 11 million messages, with ground truth available, we show that multiple machine learning models are able to reliably link those identifiers. The best of them achieves an impressive true positive rate of over 0.8 and a false positive rate of 0.001.

Related publication: [5]

8.1.4 Generalizable Features for Anonymizing Motion Signals Based on the Zeros of the Short-Time Fourier Transform

Participants: Pierre Rougé, Ali Moukadem, Alain Dieterlen, Antoine Boutet, Carole Frindel.

Thanks to the recent development of sensors and Internet of Things (IoT), it is now common to use mobile application to monitor health status. These applications rely on sensors embedded in the smartphones that measure several physical quantities such as acceleration or angular velocity. However, these data are private information that can be used to infer sensitive attributes. This contribution presents a new approach to anonymize the motion sensor data, preventing the re-identification of the user based on a selection of handcrafted features extracted from the distribution of zeros of the Shot-Time Fourier Transform (STFT). This work is motivated by recent works which highlight the importance of the zeros of the STFT ([Flandrin 2015]) and link them in the case of white noise to Gaussian Analytical Functions (GAF) ([Bardenet 2020]) where the distribution of their zeros is formally described. The proposed approach is compared with an extension of an earlier work based on filtering in the time-frequency plane and doing the classification task based on convolutional neural networks, for which we improved the evaluation method and investigated the benefits of gyroscopic sensor's data. An extensive comparison is performed on a first public dataset to assess the accuracy of activity recognition and user re-identification. We showed not only that the proposed method gives better results in term of activity/identity recognition trade-off compared with the state of the art but also that it can be generalized to other datasets.

Related publication: [8]

8.2 On the topic of privacy considerations in Machine Learning

8.2.1 MixNN: Protection of Federated Learning Against Inference Attacks by Mixing Neural Network Layers

Participants: Thomas Lebrun, Jan Aalmoes, Adrien Baud, Antoine Boutet.

Machine Learning (ML) has emerged as a core technology to provide learning models to perform complex tasks. Boosted by Machine Learning as a Service (MLaaS), the number of applications relying on ML capabilities is ever increasing. However, ML models are the source of different privacy violations through passive or active attacks from different entities. In this contribution, we present MixNN a proxy-based privacy-preserving system for federated learning to protect the privacy of participants against a curious or malicious aggregation server trying to infer sensitive information (i.e., membership and attribute inferences). MixNN receives the model updates from participants and mixes layers between participants before sending the mixed updates to the aggregation server. This mixing strategy drastically reduces privacy leaks without any trade-off with utility. Indeed, mixing the updates of the model has no impact on the result of the aggregation of the updates computed by the server. We report on an extensive evaluation of MixNN using several datasets and neural networks architectures to quantify privacy leakage through membership and attribute inference attacks as well the robustness of the protection. We show that MixNN significantly limits both the membership and attribute inferences compared to a baseline using model compression and noisy gradient (well known to damage the utility) while keeping the same level of utility as classic federated learning.

Related publication: [4]

8.2.2 Inferring Sensitive Attributes from Model Explanations

Participants: Vasisht Duddu, Antoine Boutet.

Model explanations provide transparency into a trained machine learning model's blackbox behavior to a model builder. They indicate the influence of different input attributes to its corresponding model prediction. The dependency of explanations on input raises privacy concerns for sensitive user data. However, current literature has limited discussion on privacy risks of model explanations. We focus on the specific privacy risk of attribute inference attack wherein an adversary infers sensitive attributes of an input (e.g., Race and Sex) given its model explanations. We design the first attribute inference attack against model explanations in two threat models where model builder either (a) includes the sensitive attributes in training data and input or (b) censors the sensitive attributes by not including them in the training data and input. We evaluate our proposed attack on four benchmark datasets and four state-of-the-art algorithms. We show that an adversary can successfully infer the value of sensitive attributes from explanations in both the threat models accurately. Moreover, the attack is successful even by exploiting only the explanations corresponding to sensitive attributes. These suggest that our attack is effective against explanations and poses a practical threat to data privacy. On combining the model predictions (an attack surface exploited by prior attacks) with explanations, we note that the attack success does not improve. Additionally, the attack success on exploiting model explanations is better compared to exploiting only model predictions. These suggest that model explanations are a strong attack surface to exploit for an adversary.

Related publication: [1]

8.2.3 Towards Privacy Aware Deep Learning for Embedded Systems

Participants: Thomas Lebrun, Jan Aalmoes, Adrien Baud, Antoine Boutet.

Memorization of training data by deep neural networks enables an adversary to mount successful membership inference attacks. Here, an adversary with blackbox query access to the model can infer whether an individual's data record was part of the model's sensitive training data using only the output predictions. This violates the data confidentiality, by inferring samples from proprietary training data, and privacy of the individual whose sensitive record was used to train the model. This privacy threat is profound in commercial embedded systems with on-device processing. Addressing this problem requires neural networks to be inherently private by design while conforming to the memory, power and computation constraints of embedded systems. This is lacking in literature. We present the first work towards membership privacy by design in neural networks while reconciling privacy-accuracy-efficiency trade-offs for embedded systems. We conduct an extensive privacy-centered neural network design space exploration to understand the membership privacy risks of well adopted state-of-the-art techniques: model compression via pruning, quantization, and off-the-shelf efficient architectures. We study the impact of model capacity on memorization of training data and show that compressed models (after retraining) leak more membership information compared to baseline uncompressed models while off-the-shelf architectures do not satisfy all efficiency requirements. Based on these observations, we identify quantization as a potential design choice to address the three dimensional trade-off. We propose Gecko training methodology where we explicitly add resistance to membership inference attacks as a design objective along with memory, computation, and power constraints of the embedded devices. We show that models trained using Gecko are comparable to prior defences against blackbox membership attacks in terms of accuracy and privacy while additionally providing efficiency. This enables Gecko models to be deployed on embedded systems while providing membership privacy.

Related publication: [13]

8.3 On the topic of Machine Learning and Regulation

8.3.1 Mapping the Use of Facial Recognition in Public Spaces in Europe

Participants: Claude Castelluccia, Daniel Le Métayer.

How to regulate the use of facial recognition in public spaces in Europe? This crucial debate has often been characterised by a lack of clarity and precision. In the context of the AI-regulation MIAI Chair, the authors have been working on 6 Reports to analyse the different ways in which facial recognition is being used and the related legal issues.

The first report presents the political landscape, dives into definitions of key terms and explains the project's main objectives and methodological tools, which led to the selection – and detailed study – of 25 representative cases.

The second report provides a path to understanding with a classification table presenting in the most accessible way the different facial processing functionalities and applications used in public spaces.

The 3rd Report should be of great interest to lawyers interested in data protection; AI ethics specialists; the private sector; data controllers; DPAs and the EDPB; policymakers; and the general public, who will find here an accessible way to understand all these issues.

Three additional reports are expected on other aspects of AI regulation.

Related website: ai-regulation.com

Related publications: [22] [23]

8.4 On the topic of privacy and legal considerations

8.4.1 Can Authoritative Governments Abuse the Right to Access?

Participants: Cedric Lauradoux, Cristiana Santos.

Since the application of the GDPR, legal scholars and computer scientists have identified several issues with the right of access:

- Organizations are not prepared to answer subject access requests (see [AD18]);

- Organizations are using weak methods to verify subject access requests;
- European Data Protection Authorities(DPAs) are providing different recommendations and they request non proportional or unnecessary documents to verify the identity of the requester.

We note that the EDPB guidelines address the first two issues. We hope that these Guidelines will shape and homogenize the recommendations published by all European DPAs in their websites and help in the complaining process. Whereas the present guidelines consist of a significant step to the exercise of the right of access, they need to clarify several important elements discussed in the following sections.

Related publications: [16] [3]

9 Partnerships and cooperations

Participants: all team members.

9.1 International initiatives

9.1.1 Inria associate team not involved in an IIL or an international program

MAGPIE

Title: Machine Learning and privacy challenges

Duration: 2022 to 2024 (3 years)

Coordinator: Emiliano De Cristofaro (e.decristofaro@ucl.ac.uk)

Partners:

- University College London (UCL), UK

Inria contact: Mathieu Cunche

Summary: 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.

9.1.2 Participation in other International Programs

Pack Ambition International / Face Foundation TJF

Title: *Trusty IA: Enabling Privacy Preserving in Federated Learning*

Duration: 2021 - *(2023)*

Coordinator: Antoine Boutet

Partners: University de Pennsylvanie

Inria contact: Antoine Boutet

Summary: 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.

9.2 International research visitors

9.2.1 Visits of international scientists

Other international visits to the team

Prof. Youakim Badr

Institution of origin: Univ. of Pennsylvanie, USA

Dates: from June 22nd to July 22nd, then in December 2022

Prof. Prasenjit Mitra

Institution of origin: Univ. of Pennsylvanie, USA

Dates: December 2022

9.2.2 Visits to international teams

Research stays abroad

persJanAalmoes

Visited institution: UQAM, Montréal, Quebec, Canada

Dates: March and May 2022

Context of the visit: Visit to Sébastien Gambs

9.3 European initiatives

9.3.1 H2020 projects

SPARTA

Title: Special projects for advanced research and technology in Europe

Duration: From February 1, 2019 to June 30, 2022

Coordinator: *Commissariat à l'Energie Atomique et aux Energies Alternatives (CEA), France*

Partners:

- Commissariat à l'Energie Atomique et aux Energies Alternatives (leader)
- 43 other partners (not listed here), including Inria and INSA.

Inria contact: Thomas Jensen

Summary: SPARTA will launch and execute four programs validating the operation of the network and performing ground-breaking advances in key areas for Europe's strategic autonomy:

- Full Spectrum Situational Awareness;
- Continuous Assessment in Polymorphous Environments;
- High-Assurance Intelligent Infrastructure Toolkit;
- Secure and Fair AI Systems for Citizen.

See SPARTA project description on cordis.europa.eu.

9.3.2 Other european programs/initiatives

PIVOT

- Title: Privacy-Integrated design and Validation in the constrained IoT
- Type: German-French joint call on cybersecurity - ANR - Bundesministerium für Buildung und Forschung
- Duration: 2021 - 2024
- Coordinator: French coordinator: AFNIC, German coordinator: Freie Universität Berlin
- Others partners: Hamburg Univ of Applied Science, Lobaro Industrial Solutions, INSA Lyon, Inria
- Abstract: The overall objective of the PIVOT project lies in assuring privacy of data and metadata in the Internet of Things (IoT). PIVOT will consider both low-end devices and low-power radio networks of the ultra-constrained IoT. The project will focus on four core goals: 1. A cryptographic framework for privacy-friendly service primitives on ultra-constrained IoT devices; 2. Protocols that integrate decentralized object security; 3. Minimal trust anchor provisioning on IoT devices to enable object security; 4. And multi-stakeholder name management that preserves privacy requirements and generates, allocates, and resolves names globally, regardless of the IoT applications or networks. A demonstrator based on RIOT will verify our solutions in ultraconstrained IoT networks such as LoRaWAN.

9.4 National initiatives

9.4.1 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).

9.4.2 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
- Claude Castelluccia is "Commissaire CNIL" since August 2021. Liste des commissaires CNIL

9.4.3 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.

9.4.4 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.

10 Dissemination

Participants: all team members.

10.1 Promoting scientific activities

10.1.1 Scientific events: organisation

General chair, scientific chair

- Nataliia Bielova is a co-president of the *CNIL-Inria Privact Protection Award 2022*
- Antoine Boutet organized the 6th edition of the GDR RSD / ASF Winter School on Distributed Systems and Networks 2022

Member of the organizing committees

- Nataliia Bielova has co-organized with the LINC service of the CNIL the 1st edition of *Privacy Research Day* at the CNIL, June 2022.

10.1.2 Scientific events: selection

Member of the conference program committees

- Nataliia Bielova was a member of Program Committee/Editorial Board of *Privacy Enhancing Technologies Symposium (PETs'22)*.
- Mathieu Cunche , Antoine Boutet and Vincent Roca are members of the program committee of the 12th edition of *"Atelier sur la Protection de la Vie Privée"*, June 2022.

- Mathieu Cunche is a member of Program Commitee of ACM Wisec 2022
- Mathieu Cunche is a member of Program Commitee DPM 2022
- Mathieu Cunche is a member of Program Commitee AlgoTel 2022
- Antoint Boutet was member of the Location Privacy Workshop (LPW), hosted by the IEEE Symposium on Security and Privacy, June 2022

Reviewer

- Antoine Boutet: IEEE Trans. on Dependable and Secure Computing 2022, PLOS ONE 2022

10.1.3 Invited talks

- Claude Castelluccia was invited by the Académie Nationale de Médecine for the "Médecine et IA" special day, on the occasion of the publication of the collective book "Médecine et intelligence artificielle", CNRS édition, directed by B. Nordlinger, C. Villani and O. de Fresnoye, May 2022. Suject of the contribution: "Online Brain Hacking"
- Vincent Roca was invited by the Académie Nationale de Médecine for the "Médecine et IA" special day, on the occasion of the publication of the collective book "Médecine et intelligence artificielle", CNRS édition, directed by B. Nordlinger, C. Villani and O. de Fresnoye, May 2022. Suject of the contribution: "TousAntiCovid : gros plan sur les deux protocoles de traçage numérique"
- Vincent Roca, "Digital contact/presence tracing in FR/Europe: lessons learned after two years", talk during the PRIVASKI seminar, March 2022.
- Vincent Roca, "Web and privacy: where do we go and what do we want?", invited talk during the STIC AmSud Scientific Seminar, October 2022.
- Vincent Roca, round table "Souveraineté Numérique et Vie Privée, entre contrôle et respect des données", 12ème Atelier sur la Protection de la Vie Privée (APVP 2022), June 2022.
- Antoine Boutet, "Inférence d'informations sensibles dans l'apprentissage automatique et contre mesures", GT-PVP seminar, September 2022
- Antoine Boutet, "Vers une protection à la source des informations capteurs pour se prémunir des inférences d'informations sensibles", FIL seminar, April 2022
- Antoine Boutet, "DYSAN: dynamically sanitizing motion sensor data against sensitive inferences through adversarial networks", French-Japan Cybersecurity Workshop, March 2022

10.1.4 Leadership within the scientific community

- Mathieu Cunche, co-chair of the Privacy Protection (PVP) Working Group of *GDR Sécurité*
- Nataliia Bielova, member of the Steering Committee of Atelier sur la Protection de la Vie Privée (APVP)
- Antoine Boutet, chair of the Privacy Protection Working Group of the French-Japan Cybersecurity Collaboration

10.2 Responsibilities in Public Authorities

- Claude Castelluccia was nominated at the CNIL (French Data Protection Agency) as one of its commissioners , August 2021.
- Nataliia Bielova has joined the CNIL (French Data Protection Authority) for 1 year as *Senior Privacy Fellow*, September 2021.

10.3 Standardisation activities

- Vincent Roca is co-chair of the "Coding for Efficient Network Communications" (NWCRG) Internet Research Task Force (IRTF): (nwcrg site).
- Vincent Roca is member and reviewer of the IETF Security Directorate (SecDir), and member of the Internet Research Steering Group (IRSG). (IETF site).
- Mathieu Cunche is Delegate chair of the "MAC Address Device Identification for Network and Application Services" (MADINAS) IETF Working Group. (madinas site).

10.4 Teaching - Supervision - Juries

10.4.1 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).

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.

10.4.2 Supervision

PhD defended in 2022: None

On-going PhDs:

- Coline Boniface, (Sept. 2019 -) *"Attribution of cyber attacks"*, co-supervised by Cédric Lauradoux and Karine Bannelier
- Michael Toth (Dec. 2019 -), co-supervised by Nataliia Bielova and Vincent Roca
- Samuel Pelissier, (Sept. 2021 -), co-supervised by Mathieu Cunche and Vincent Roca
- Suzanne Lansade, (Oct. 2020 -), co-supervised by Cédric Lauradoux and Vincent Roca
- Jan Aalmoes, (Sept. 2021 -), co-supervised by Antoine Boutet, Carole Frindel and Mathieu Cunche
- Thomas Lebrun, (Oct. 2021 -), co-supervised by Antoine Boutet, Claude Castellucccia and Mathieu Cunche

New PhDs:

- Gilles Mertens, (Nov. 2022 -), *"Progressive Web Apps"*, co-supervised by Vincent Roca and Mathieu Cunche
- Teodora Curelariu, (Dec. 2022 -), *"Cyber-incidents entre monde prive‘ et public"*, co-supervised by Cédric Lauradoux and Karine Bannelier

10.4.3 Juries

- Vincent Roca was examiner for the PhD defense of Tomas Conception Miranda, "Profiling and Visualizing Android Malware Datasets", November 2022.
- Nataliia Bielova was a member of PhD defense of Hanaa Alshareef, Chalmers University of Technology (SE), August 2022.
- Nataliia Bielova was a member of the PhD thesis supervision commitee of Emre Kocyigit, University of Luxembourg (LU), 2022.
- Nataliia Bielova was a member of the Comprehensive exam committee of Maaz Bin Musa, University of Iowa (US), 2022.
- Mathieu Cunche was examiner for the PhD defense of Robin Carpentier, "Privacy-preserving third-party computations on secure personal data management systems", Université de Versailles-Saint-Quentin-en-Yvelines, December 2022
- Mathieu Cunche was reviewer for the PhD defense of Andy Amoordon, "Méthodes de détection d'attaques cybernétiques par une surveillance multicouches de communication", Université de Lille December 2022

- Mathieu Cunche was reviewer for the PhD defense of Héber Hwang Arcolezi, "Production de Données Catégorielles Respectant la Confidentialité Différentielle Conception et Applications au Apprentissage Automatique", Université de Franche-Comté, January 2022
- Antointe Boutet was reviewer for hte PhD defense of Lestyan Szilvia, "Privacy of Vehicular Time Series Data", June 2022

10.5 Popularization

10.5.1 Interventions

- Nataliia Bielova was interviewed in *LeMonde.fr* on their large-scale detection of Web tracking, cookie syncing and browser fingerprinting, and development of ERNIE extension, 2022.
- Nataliia Bielova was interviewed in *Wired.com* about the advances in the field of Browser Fingerprinting based on her journal article at ACM TWEB, 2022.
- Mathieu Cunche was a guest on RFI, Le débat du jour : Sommes-nous condamnés à être espionnés?, 16/06/22
- Mathieu Cunche was a guest on RTBF, Les éclaireurs : "Totale connexion !", 02/04/22
- Mathieu Cunche was interviewed in the podcast Monde Numérique, Vous allez tout comprendre : le Wi-Fi, 06/08/22
- Mathieu Cunche was interviewed in Imagine, Totale connexion, 03/01/22 , N° 149 / mars-avril 2022
- Mathieu Cunche was interviewed in Femme Actuelle, Je protège mes données personnelles, 03/02/2022

11 Scientific production

11.1 Major publications

[1] V. Duddu and A. Boutet. 'Inferring Sensitive Attributes from Model Explanations'. In: CIKM 2022 - 31st ACM International Conference on Information and Knowledge Management. Atlanta / Hybrid, United States, 17th Oct. 2022, pp. 1–10. URL: https://hal.inria.fr/hal-03781528.

[2] I. Fouad, C. Santos, A. Legout and N. Bielova. 'My Cookie is a phoenix: detection, measurement, and lawfulness of cookie respawning with browser fingerprinting'. In: PETS 2022 - 22nd Privacy Enhancing Technologies Symposium. Sydney, Australia, 11th July 2022. URL: https://hal.science/hal-03218403.

[3] C. Lauradoux and C. Santos. *Feedbacks on Guidelines 01/2022 on data subject rights -Right of access.* 11th Mar. 2022. URL: https://hal.inria.fr/hal-03957253.

[4] T. Lebrun, A. Boutet, J. Aalmoes and A. Baud. 'MixNN: Protection of Federated Learning Against Inference Attacks by Mixing Neural Network Layers'. In: MIDDLEWARE 2022 - 23rd ACM/IFIP International Middleware Conference. Quebec, Canada, 7th Nov. 2022, pp. 1–11. DOI: 10.1145/3528535.3565240. URL: https://hal.inria.fr/hal-03795818.

[5] S. Pélissier, M. Cunche, V. Roca and D. Donsez. 'Device re-identification in LoRaWAN through messages linkage'. In: WiSec 2022 - 15th ACM Conference on Security and Privacy in Wireless and Mobile Networks. San Antonio, TX, United States: ACM, 16th May 2022, pp. 1–6. URL: https://hal.inria.fr/hal-03624160.

[6] M. Toth, N. Bielova and V. Roca, eds. *On dark patterns and manipulation of website publishers by CMPs.* Vol. 2022. 3. PoPETs, a self-published open access journal, 2022, pp. 478–497. DOI: 10.56553/popets-2022-0082. URL: https://hal.inria.fr/hal-03577024.

11.2 Publications of the year

International journals

[7] M. Ienca, J. J. Fins, R. J. Jox, F. Jotterand, S. Voeneky, R. Andorno, T. Ball, C. Castelluccia, R. Chavarriaga, H. Chneiweiss, A. Ferretti, O. Friedrich, S. Hurst, G. Merkel, F. Molnár-Gábor, J.-M. Rickli, J. Scheibner, E. Vayena, R. Yuste and P. Kellmeyer. 'Towards a Governance Framework for Brain Data'. In: *Neuroethics* 15 (3rd June 2022). DOI: 10.1007/s12152-022-09498-8. URL: https://hal.inria.fr/hal-03956305.

[8] P. Rougé, A. Moukadem, A. Dieterlen, A. Boutet and C. Frindel. 'Generalizable Features for Anonymizing Motion Signals Based on the Zeros of the Short-Time Fourier Transform'. In: *Journal of Signal Processing Systems* (25th July 2022), pp. 1–14. DOI: 10.1007/s11265-022-01798-9. URL: https://hal.inria.fr/hal-03781980.

[9] M. Toth, N. Bielova and V. Roca. 'On dark patterns and manipulation of website publishers by CMPs'. In: *Proceedings on Privacy Enhancing Technologies (PoPETs)* 2022.3 (2022), pp. 478–497. DOI: 10.56553/popets-2022-0082. URL: https://hal.inria.fr/hal-03577024.

International peer-reviewed conferences

[10] C. Adam and C. Lauradoux. 'A serious game for debating about the use of Artificial Intelligence during the COVID-19 pandemic'. In: 19th International Conference on Information Systems for Crisis Response and Management, ISCRAM 2022. Tarbes, France, 22nd May 2022. URL: https://hal.inria.fr/hal-03957229.

[11] S. Adhatarao and C. Lauradoux. 'Robust PDF Files Forensics Using Coding Style'. In: ICT Systems Security and Privacy Protection - 37th IFIP TC 11 International Conference, SEC 2022. Vol. 648. IFIP Advances in Information and Communication Technology. Copenhagen, France: Springer International Publishing, 3rd June 2022, pp. 179–195. DOI: 10.1007/978-3-031-06975-8_11. URL: https://hal.inria.fr/hal-03957159.

[12] V. Duddu and A. Boutet. 'Inferring Sensitive Attributes from Model Explanations'. In: CIKM 2022 - 31st ACM International Conference on Information and Knowledge Management. Atlanta / Hybrid, United States, 17th Oct. 2022, pp. 1–10. URL: https://hal.inria.fr/hal-03781528.

[13] V. Duddu, A. Boutet and V. Shejwalkar. 'Towards Privacy Aware Deep Learning for Embedded Systems'. In: SAC 2022 - 37th ACM/SIGAPP Symposium on Applied Computing. Virtual, France: ACM, 25th Apr. 2022, pp. 520–529. URL: https://hal.inria.fr/hal-03781979.

[14] I. Fouad, C. Santos, A. Legout and N. Bielova. 'My Cookie is a phoenix: detection, measurement, and lawfulness of cookie respawning with browser fingerprinting'. In: PETS 2022 - 22nd Privacy Enhancing Technologies Symposium. Sydney, Australia, 11th July 2022. URL: https://hal.archives-ouvertes.fr/hal-03218403.

[15] N. Grgić-Hlača, C. Castelluccia and K. P. Gummadi. 'Taking Advice from (Dis)Similar Machines: The Impact of Human-Machine Similarity on Machine-Assisted Decision-Making'. In: HCOMP 2022 - The Tenth AAAI Conference on Human Computation and Crowdsourcing. Virtual, France, 6th Nov. 2022. URL: https://hal.inria.fr/hal-03956115.

[16] C. Lauradoux. 'Can Authoritative Governments Abuse the Right to Access?' In: Annual Privacy Forum 2022. Vol. 13279. Lecture Notes in Computer Science. Varsovie (PL), Poland: Springer International Publishing, 20th May 2022, pp. 23–33. DOI: 10.1007/978-3-031-07315-1_2. URL: https://hal.inria.fr/hal-03957151.

[17] T. Lebrun, A. Boutet, J. Aalmoes and A. Baud. 'MixNN: Protection of Federated Learning Against Inference Attacks by Mixing Neural Network Layers'. In: MIDDLEWARE 2022 - 23rd ACM/IFIP International Middleware Conference. Quebec, Canada, 7th Nov. 2022, pp. 1–11. DOI: 10.1145/3528535.3565240. URL: https://hal.inria.fr/hal-03795818.

[18] 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.

[19] S. Pélissier, M. Cunche, V. Roca and D. Donsez. 'Device re-identification in LoRaWAN through messages linkage'. In: WiSec 2022 - 15th ACM Conference on Security and Privacy in Wireless and Mobile Networks. San Antonio, TX, United States: ACM, 16th May 2022, pp. 1–6. URL: https://hal.inria.fr/hal-03624160.

National peer-reviewed Conferences

[20] A. Boutet and G. Derache. 'Simulation de crise -24h dans la tempête'. In: RESSI 2022 - Rendez-vous de la Recherche et de l'Enseignement de la Sécurité des Systèmes d'Information. Chambon-sur-Lac, France, 10th May 2022, pp. 1–4. URL: https://hal.inria.fr/hal-03611184.

Scientific book chapters

[21] V. Roca. 'TousAntiCovid : gros plan sur les deux protocoles de traçage numérique de l'application'. In: *Médecine et intelligence artificielle.* CNRS Editions, 24th Mar. 2022, pp. 1–5. URL: https://hal.inria.fr/hal-03618394.

Reports & preprints

[22] T. Christakis, K. Bannelier, C. Castelluccia and D. Le Métayer. *MAPPING THE USE OF FACIAL RECOGNITION IN PUBLIC SPACES IN EUROPE A QUEST FOR CLARITY: UNPICKING THE "CATCH-ALL" TERM.* May 2022. Université Grenoble Alpes (UGA); Centre d'Etudes sur la Sécurité Internationale et les Coopérations Européennes (CESICE), May 2022. URL: https://hal.inria.fr/hal-03956132.

[23] T. Christakis, K. Bannelier-Christakis, C. Castelluccia and D. Le Métayer. *Facial recognition for authorisation purposes (part 3).* Université Grenoble Alpes (UGA), May 2022. URL: https://hal.inria.fr/hal-03956166.

[24] G. Kessibi, A. O. Hamouda, C. Poirier and A. Boutet. *A complementary utility and privacy trade-off evaluation of Google's FloC API.* 25th May 2022. URL: https://hal.inria.fr/hal-03953308.

[25] V. Roca. *Digital contact/presence tracing in FR/Europe: lessons learned after two years.* 8th Mar. 2022. URL: https://hal.inria.fr/hal-03693797.

Other scientific publications

[26] J. Hugon, M. Cunche and T. Begin. 'RoMA: Rotating MAC Address for privacy protection'. In: SIGCOMM 2022 - 36th Conference of the ACM Special Interest Group on Data Communication – Poster Session. Amsterdam, Netherlands, 22nd Aug. 2022. DOI: 10.1145/3546037.3546055. URL: https://hal.inria.fr/hal-03778273.

[27] C. Lauradoux and C. Santos. *Feedbacks on Guidelines 01/2022 on data subject rights -Right of access.* 11th Mar. 2022. URL: https://hal.inria.fr/hal-03957253.

11.3 Other

Scientific popularization

[28] M. Cunche. 'Le traçage cyberphysique des personnes et la vie privée'. In: *Interstices* (28th Jan. 2022). URL: https://hal.inria.fr/hal-03589575.