Differential Privacy
NGI Porto - 2018

Gustavo Viqueira
Manuel Noya
Palo Alto (CA) & A Coruña (Spain)
Sept 2018
Our credentials

We founded Linknovate en 2012 in Stanford University, CA. We have been awarded 3 EU projects (grants) by the EC and have gone through 2 of the most prestigious startup accelerators in the world.

Some of our satisfied clients:
Differential Privacy

https://www.linknovate.com/search/?query=%22differential+privacy%22,%22privacy+by+design%22
Insights from Linknovate.com


Analysis of organisations behind these references show that small medium size companies are starting to pave the way. Clear sign of market readiness and industrial interest.
The type of data source that has been more important in the last 8 years are “conference proceedings”, typical of R&D&I in ICT. Low number of patent applications indicates opportunity and news indicate the above mentioned market readiness.

As saw in previous slide Universities have led research in the area for the last 10 years, however SMEs have been active and are now the ones who contribute the most in terms of activity.
Public funding trends.
EU investing more than UK and US in this area, even though main research organizations in the topic are US-based. Average investing per year around 20-25M, and interestingly enough: *decreasing from the peak in 2012-2013.*

Document cluster trends.
Shows related topics and subtopics.
Country activity segmentation.
US similar activity to EU countries plus UK, combined. China already second, primarily with academic organisations.

Trends looking at particular organisations shows Microsoft traditional interest in the area, Apple's new interest, and 2 academic institutions to compare with: Upenn (highest activity in 2014-2016) and Wuhan Univ. (most active in 2017-2018).
# Ranking of Active Entities Worldwide

<table>
<thead>
<tr>
<th>Ranking</th>
<th>Name</th>
<th>Score</th>
<th>Pub</th>
<th>Con</th>
<th>Gra</th>
<th>Pat</th>
<th>Tra</th>
<th>New</th>
<th>Web</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Microsoft</td>
<td>144.4</td>
<td>13</td>
<td>52</td>
<td>-</td>
<td>4</td>
<td>-</td>
<td>14</td>
<td>-</td>
</tr>
<tr>
<td>2</td>
<td>SAP</td>
<td>90.9</td>
<td>-</td>
<td>4</td>
<td>-</td>
<td>3</td>
<td>-</td>
<td>1</td>
<td>-</td>
</tr>
<tr>
<td>3</td>
<td>Apple Inc</td>
<td>90.6</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>1</td>
<td>-</td>
<td>2</td>
<td>-</td>
</tr>
<tr>
<td>4</td>
<td>Wuhan University</td>
<td>74.9</td>
<td>11</td>
<td>6</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>5</td>
<td>University of Pennsylvania</td>
<td>73.5</td>
<td>6</td>
<td>41</td>
<td>4</td>
<td>-</td>
<td>-</td>
<td>1</td>
<td>-</td>
</tr>
<tr>
<td>6</td>
<td>Pennsylvania State University</td>
<td>63.1</td>
<td>11</td>
<td>24</td>
<td>3</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>

- **Grant | Synergy: Collaborative: Security and Privacy-Aware Cyber-Physical Systems**
- **Publication | Differential privacy preserving method for trajectory clustering**
- **Publication | Enhancing Selectivity in Big Data**
### Ranking of Active Entities Worldwide (II)

<table>
<thead>
<tr>
<th>Ranking</th>
<th>Name</th>
<th>Score</th>
<th>Pub</th>
<th>Con</th>
<th>Gra</th>
<th>Pat</th>
<th>Tra</th>
<th>New</th>
<th>Web</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>Harvard University</td>
<td>60.0</td>
<td>6</td>
<td>33</td>
<td>1</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>8</td>
<td>Carnegie Mellon University</td>
<td>56.3</td>
<td>13</td>
<td>23</td>
<td>2</td>
<td>-</td>
<td>-</td>
<td>1</td>
<td>-</td>
</tr>
<tr>
<td>9</td>
<td>Emory University</td>
<td>55.6</td>
<td>16</td>
<td>26</td>
<td>3</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>10</td>
<td>University of Illinois at Urbana - Champaign</td>
<td>47.6</td>
<td>9</td>
<td>16</td>
<td>4</td>
<td>-</td>
<td>-</td>
<td>1</td>
<td>-</td>
</tr>
<tr>
<td>11</td>
<td>Purdue University</td>
<td>47.0</td>
<td>6</td>
<td>20</td>
<td>3</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>12</td>
<td>Cornell University</td>
<td>46.7</td>
<td>4</td>
<td>20</td>
<td>6</td>
<td>-</td>
<td>-</td>
<td>1</td>
<td>-</td>
</tr>
</tbody>
</table>

- Grant | SaTC: CORE: Medium: Collaborative: Contextual Integrity: From Theory to Practice
- Publication | A Two-Phase Algorithm for Differentially Private Frequent Subgraph Mining
- Conference | Finite sample differentially private confidence intervals
Relevant References
<table>
<thead>
<tr>
<th>Title</th>
<th>Abstract</th>
<th>Affiliation</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Individual differential privacy: A utility-preserving formulation of differential privacy guarantees</td>
<td>We propose individual differential privacy, an alternative differential privacy notion that offers the same privacy guarantees as standard differential privacy to individuals (even though not to groups of individuals). This new notion allows the data controller to adjust the distortion to the actual data set, which results in less distortion and more analytical accuracy.</td>
<td>Rovira i Virgili University</td>
<td>+info</td>
</tr>
<tr>
<td>Protecting personal trajectories of social media users through differential privacy</td>
<td>This paper proposes an innovative private trajectories release model and associated algorithms with differential privacy guarantees that considers both data privacy and data utility.</td>
<td>University of Melbourne</td>
<td>+info</td>
</tr>
<tr>
<td>Minimax filter: Learning to preserve privacy from inference attacks</td>
<td>The paper proposes a novel filter-based mechanism which preserves privacy of continuous and high-dimensional attributes against inference attacks. Finding the optimal utility-privacy tradeoff is formulated as a min-diff-max optimization problem.</td>
<td>Ohio State University</td>
<td>+info</td>
</tr>
<tr>
<td>Differential privacy and generalization: Sharper bounds with applications</td>
<td>In this paper we deal with the problem of improving the recent milestone results on the estimation of the generalization capability of a randomized learning algorithm based on Differential Privacy (DP). In particular, we derive new DP based multiplicative Chernoff and Bennett type generalization bounds, which improve over the current state-of-the-art Hoeffding type bound.</td>
<td>University of Genoa</td>
<td>+info</td>
</tr>
<tr>
<td>The necessity of the implementation of Privacy by Design in sectors where data protection concerns arise</td>
<td>This article examines the extent to which Privacy by Design can safeguard privacy and personal data within a rapidly evolving society. This paper will first briefly explain the theoretical concept and the general principles of Privacy by Design, as laid down in the General Data Protection Regulation. Then, by indicating specific examples of the implementation of the Privacy by Design approach, it will be demonstrated why the implementation of Privacy by Design is a necessity in a number of sectors where specific data protection concerns arise (biometrics, e-health and video-surveillance) and how it can be implemented.</td>
<td>Athens Law Bar</td>
<td>+info</td>
</tr>
<tr>
<td>Opening the black box: Petri nets and Privacy by Design</td>
<td>Building on the growing literature in algorithmic accountability, this paper investigates the use of a process visualisation technique known as the Petri net to achieve the aims of Privacy by Design.</td>
<td>University of Edinburgh</td>
<td>+info</td>
</tr>
<tr>
<td>Location Privacy Protection Based on Differential Privacy Strategy for Big Data in Industrial Internet of Things</td>
<td>We propose a location privacy protection method that satisfies differential privacy constraint to protect location data privacy and maximizes the utility of data and algorithm in Industrial IoT.</td>
<td>Nanjing University of Information Science and Technology</td>
<td>+info</td>
</tr>
</tbody>
</table>
# Some relevant patents

<table>
<thead>
<tr>
<th>Title</th>
<th>Description</th>
<th>Status</th>
<th>Entity</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Differentially Private Processing And Database Storage</td>
<td>The hardware database privacy device receives a request from a client device to perform a query of the private database system and identifies a level of differential privacy corresponding to the request.</td>
<td>Application</td>
<td>LeapYear Technologies Inc.</td>
<td>+info</td>
</tr>
<tr>
<td>Privacy By Design Database And Methods Operating Thereon</td>
<td>An apparatus for preserving streaming data anonymity, the apparatus comprising a memory configured to store streaming data comprising a first data set and at least one processor operably connected to the memory, the at least one processor configured to transform the first data set to a second data set based on a difference level for preserving differential privacy of the first data set.</td>
<td>Application</td>
<td>Aztrix Nv</td>
<td>+info</td>
</tr>
<tr>
<td>Differential Privacy For Message Text Content Mining</td>
<td>Systems and methods are disclosed for determining whether a message received by a client may be spam, in a computing environment that preserves privacy.</td>
<td>Application</td>
<td>Apple Inc</td>
<td>+info</td>
</tr>
<tr>
<td>Differential Privacy And Outlier Detection Within A Non-Interactive Model</td>
<td>A system for differential privacy is provided. In some implementations, the system performs operations comprising receiving a plurality of indices for a plurality of perturbed data points, which are anonymized versions of a plurality of unperturbed data points, wherein the plurality of indices indicate that the plurality of unperturbed data points are identified as presumed outliers.</td>
<td>Application</td>
<td>SAP SE</td>
<td>+info</td>
</tr>
<tr>
<td>Privacy-Preserving Transformation Of Continuous Data</td>
<td>A data processing method receives a set of time-series user data and also receives a privacy requirement of the time-series user data. Next, the time-series user data is transformed using the privacy requirement such that the transforming satisfies differential privacy.</td>
<td>Application</td>
<td>Samsung Electronics Co Ltd</td>
<td>+info</td>
</tr>
<tr>
<td>Method For Differentially Private Aggregation In A Star Topology Under A Realistic Adversarial Model</td>
<td>One embodiment provides a system for noise addition to enforce data privacy protection in a star network. In operation, participants may add a noise component to a dataset. An aggregator may receive the noise components from the plurality of participants, compute an overall noise term based on the received noise components, and aggregate values using the noise components and overall noise term.</td>
<td>Application</td>
<td>Palo Alto Research Center Inc</td>
<td>+info</td>
</tr>
</tbody>
</table>
Relevant Organisations
Microsoft has several publications and patents about geometric response systems to preserve privacy, and also about algorithms to maintain the privacy of the user of CPS systems.

The SAP company has several patents and publications related to systems of detection of atypical values that preserve privacy for data flows, and also with encrypted database systems.

IBM has several publications related to active learning statistical algorithms for noise tolerance and differential privacy, optimal mechanisms for randomized response in differential privacy and also systems enabled to work in fog, such as PPFA: Privacy Preserving Fog-enabled Aggregation in Smart Grid. Participating in 2 European Projects; MIDAS and AU2EU.

Google mainly works on optimal noise adding mechanisms for approximate differential privacy.

PARTICIPATING IN 2 EUROPEAN PROJECTS
• MIDAS
• AU2EU
Other relevant organisations

The foundation Privacy by Design was developed in 2016 from the Digital Security research group of Radboud University and the Privacy and Identity Lab PI.lab. The foundation is an independent non-profit spin-off. The foundation mainly focuses on its own identity platform IRMA for privacy-friendly attribute-based authentication. The approach is based on freely available open source software.

WireWheel, Inc. develops a Data Privacy Management (DPM) platform that helps comply with data privacy and data protection regulations, including the EU GDPR, Privacy Shield, PCI DSS, and HIPAA. It combines machine learning, data science, and cloud computing.

The company raised $10.1M of funds, $7M on June 2018.
**Privitar Lens** is a “privacy-preserving query interface for reporting and statistical analysis. Privitar Lens allows analysts to perform sophisticated analytical queries of the data (e.g. counts, sums, histograms), but prevents direct access to the underlying sensitive data,” which is also known as differential privacy. On top of the products itself, Privitar logs and audits all queries.

The company raised $21.2M of funds, $16M on July 2017.

**Orchid** is a platform that aims to provide anonymized internet access to people across the globe, particularly individuals who live in countries with excessive government oversight of their browsing and shopping. Part of the point also seems to be to insulate users from the many companies that now harvest and sell their data, including walled gardens like Facebook and other giants like AT&T.

The stated goal of the **Orchid** is to provide anonymized internet access to people across the globe, particularly individuals who live in countries with excessive government oversight of their browsing and shopping. Part of the point also seems to be to insulate users from the many companies that now harvest and sell their data, including walled gardens like Facebook and other giants like AT&T.

The company raised $40.8M of funds, $36.1M on April 2018.
Other relevant organisations

**LeapYear** provides fully automated machine learning applications and developer APIs. They protect confidential, regulated, and proprietary data assets with mathematically proven security. Differential privacy, the highest standard of data protection, is embedded into every computation, so developers and analysts are never exposed to sensitive information.

*The company raised $12.6M of funds on August 2016.*

**Apple** is very involved in the use of differential privacy, as demonstrated by macOS High Sierra, that brings with it some key updates to Safari, including the ability to disable cross-site cookie tracking and turn off autoplaying ads. The company is using its differential privacy technology to gather information from user habits that will help it identify problematic websites. The new implementation is already covered by the Device Analytics program that Apple offers up when users sign into their new macOS or iOS device.
European Grants
https://www.linknovate.com/search/?query=%22differential+privacy%22,%22privacy+by+design%22&grant_origin= european&doc_type=grant
## Ranking of Active Entities Worldwide

<table>
<thead>
<tr>
<th>Ranking</th>
<th>Name</th>
<th>Score</th>
<th>Pub</th>
<th>Con</th>
<th>Gra</th>
<th>Pat</th>
<th>Tra</th>
<th>New</th>
<th>Web</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Catholic University of Leuven</td>
<td>11.5</td>
<td>-</td>
<td>-</td>
<td>5</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>2</td>
<td>Atos Spain SA</td>
<td>7.5</td>
<td>-</td>
<td>-</td>
<td>3</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>3</td>
<td>University of Cologne</td>
<td>6.9</td>
<td>-</td>
<td>-</td>
<td>1</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>4</td>
<td>Ethniko Kentro Erevnas Kai Technologikis Anaptyxis</td>
<td>6.6</td>
<td>-</td>
<td>-</td>
<td>3</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>5</td>
<td>Fraunhofer Gesellschaft Zur Foerderung der Angewandten Forschung E.V.</td>
<td>6.4</td>
<td>-</td>
<td>-</td>
<td>3</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>6</td>
<td>Technical University of Madrid</td>
<td>6.0</td>
<td>-</td>
<td>-</td>
<td>2</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>

**Grants:**

- **Grant | PRIPARE - PReparing Industry to Privacy-by-design by supporting its Application in REsearch**
- **Grant | DEFeND - Data Governance for Supporting GDPR**
- **Grant | CONNEXIONs - InterCONnected NEXt-Generation Immersive IoT Platform of Crime and Terrorism DetectiON, PredictiON, InvestigatiON, and PreventiON Services**
### Ranking of Active Entities Worldwide (II)

<table>
<thead>
<tr>
<th>Ranking</th>
<th>Name</th>
<th>Score</th>
<th>Pub</th>
<th>Con</th>
<th>Gra</th>
<th>Pat</th>
<th>Tra</th>
<th>New</th>
<th>Web</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>GridPocket SAS</td>
<td>6.0</td>
<td>-</td>
<td>-</td>
<td>2</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>8</td>
<td>Ministere de l'Interieur</td>
<td>5.9</td>
<td>-</td>
<td>-</td>
<td>3</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>9</td>
<td>Engineering Ingegneria Informatica SpA</td>
<td>5.4</td>
<td>-</td>
<td>-</td>
<td>2</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>10</td>
<td>TU Eindhoven</td>
<td>5.4</td>
<td>-</td>
<td>-</td>
<td>3</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>11</td>
<td>TRIALOG</td>
<td>5.2</td>
<td>-</td>
<td>-</td>
<td>2</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>12</td>
<td>Institute National Of Recherche En Informatique Et En Automatique</td>
<td>5.2</td>
<td>-</td>
<td>-</td>
<td>2</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>

---

**Grant | BPR4GDPR** - Business Process Re-engineering and functional toolkit for GDPR compliance

**Grant | CONNEXIONs** - InterCONnected NEXt-Generation Immersive IoT Platform of Crime and Terrorism DetectiON, PredictiON, InvestigatiON, and PreventiON Services

**Grant | DEFeND** - Data Governance for Supporting GDPR
Relevant References
<table>
<thead>
<tr>
<th>Title</th>
<th>Description</th>
<th>Coordinator or Entity Awarded</th>
<th>Data</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>DEFeND - Data Governance for Supporting GDPR</td>
<td>DEFeND platform enables building and analysing models following a Privacy-by-Design approach spanning over two levels, the Planning Level and the Operational Level, and across three management areas: Data Scope, Data Process and Data Breach. The consortium will leverage existing software, tools and methodologies towards the implementation of the platform software components.</td>
<td>ATOS SPAIN SA</td>
<td>AGENCY: European Commission AMOUNT: €3.3M YEAR: 2018 - 2020</td>
<td>+info</td>
</tr>
<tr>
<td>VISAGE - Visible Attributes through Genomics: Broadened Forensic Use of DNA for Constructing Composite Sketches from Traces</td>
<td>The VISAGE Toolkit will consider ethical, societal, and legal dimensions of Forensic DNA Phenotyping as identified within the Project, by applying a privacy-by-design strategy.</td>
<td>ERASMUS UNIVERSITAIR MEDISCH CENTRUM ROTTERDAM</td>
<td>AGENCY: SBIR - STTR AMOUNT: €5M YEAR: 2017 - 2021</td>
<td>+info</td>
</tr>
<tr>
<td>Smart Trust - Smart Trust: Secure Mobile ID for Trusted Smart Borders</td>
<td>Smart-Trust introduces a new technological enabler for Mobile ID which drastically increases the reliability and trust levels of identity verification at European borders, thus increasing the security of member states. The platform is compatible with a seamless self-service experience based on biometrics on the move which provides freedom of movements to citizens while ensuring their privacy safeguarded according to Privacy by Design principles.</td>
<td>VISION BOX - SOLUCOES DE VISAO POR COMPUTADOR SA</td>
<td>AGENCY: European Commission AMOUNT: €2.9M YEAR: 2018 - 2019</td>
<td>+info</td>
</tr>
<tr>
<td>PRI Pare - PReparing Industry to Privacy-by-design by supporting its Application in REsearch</td>
<td>The mission of PRIPARE is twofold: facilitate the application of a privacy and security -by-design methodology that will contribute to the advent of unhindered usage of Internet against disruptions, censorship and surveillance, support its practice by the ICT research community to prepare for industry practice; foster risk management culture through educational material targeted to a diversity of stakeholders.</td>
<td>TRIALOG</td>
<td>AGENCY: European Commission AMOUNT: €1.3M YEAR: 2013 - 2015</td>
<td>+info</td>
</tr>
<tr>
<td>SODA - Scalable Oblivious Data Analytics</td>
<td>SODA project will enable practical privacy-preserving analytics of information from multiple data assets using multi-party computation (MPC) techniques.</td>
<td>PHILIPS ELECTRONICS NEDERLAND B.V.</td>
<td>AGENCY: European Commission AMOUNT: €3.3M YEAR: 2017 - 2019</td>
<td>+info</td>
</tr>
</tbody>
</table>
Relevant Organisations
Atos Spain S.A. – Spain

Big Data Analytics and Privacy and Data Protection - White Paper

The rise of Big Data and Data Analytics provides great opportunities for organizations to realize new ways of doing business

Organizations that do not ‘catch the Big Data Analytics train’ run the risk of falling behind. According to the European Commission the value of European citizens’ personal data has the potential to grow to nearly €1 trillion a year by 2020.

The value of European citizens’ personal has the potential to grow to nearly €1 trillion annually by 2020.

Lawmakers around the globe, responding to many well-publicized situations and concerns expressed by citizens, have become more and more focused and concerned with privacy matters. An important development in this respect is the current reform of the European Union’s (EU) data protection legislation framework which revolves around the adoption of a new ‘General Data Protection Regulation’ (hereinafter referred to as ‘the Regulation’).

The Regulation will replace the current European Data Protection Directive (EU Directive 95/46/EC6) and was adopted in April 2016. It shall be enforced on May 25th of 2018. It will bring major changes to data protection legislation in Europe.

This White Paper explains how organizations can significantly improve their efficiency and offerings with Big Data Analytics while implementing the relevant privacy & data protection principles and rules.

PARTICIPATING IN 3 EUROPEAN PROJECTS

- DEFeND - Coordinator
- PRIPARE
- RERUM

Atos SE provides information technology services and solutions worldwide. It offers infrastructure and data management services, including cloud services and digital workplace services, business and platform solutions, big data, and cybersecurity products and services, as well as transactional services. The company’s solutions include automated help and interaction centers, cloud and mobile solutions, unified communications and collaboration tools.
Atos SE provides information technology services and solutions worldwide. It offers infrastructure and data management services, including cloud services and digital workplace services, business and platform solutions, big data, and cybersecurity products and services, as well as transactional services. The company's solutions include automated help and interaction centers, cloud and mobile solutions, unified communications and collaboration tools.

PARTICIPATING IN 3 EUROPEAN PROJECTS

- **DEFeND** - Data Governance for Supporting GDPR (Coordinator)
- **PRIPARE** - PReparing Industry to Privacy-by-design by supporting its Application in REsearch
- **RERUM** - REliable, Resilient and secUre IoT for sMart city applications

Collaboration with Technical University of Madrid, University of Vigo and Trialog among others, in a publication about engineering privacy and security by design related with the European project PRIPARE.
Atos Spain S.A. – Spain
Philips – Netherlands

Koninklijke Philips N.V. (Philips, stylized as PHILIPS) is a Dutch multinational technology company headquartered in Amsterdam currently focused in the area of healthcare. Philips is organized into three main divisions:

- Philips Consumer Lifestyle (formerly Philips Consumer Electronics and Philips Domestic Appliances and Personal Care)
- Philips Healthcare (formerly Philips Medical Systems)
- Signify N.V.
Telefónica – Spain

Telefónica, S.A. is a Spanish multinational broadband and telecommunications provider with operations in Europe, Asia, North America and South America. Operating globally, it is one of the largest mobile network providers in the world. The company started as a public telecommunications company. Its head office is in the Distrito

PARTICIPATING IN 2 EUROPEAN PROJECTS

- ENCASE - Enhancing Security And Privacy in the Social Web: a user centered approach for the protection of minors
- TYPES - Towards transparency and Privacy in the online advertising business

Telefónica, S.A. is a Spanish multinational broadband and telecommunications provider with operations in Europe, Asia, and North, Central and South America. Operating globally, it is one of the largest telephone operators and mobile network providers in the world.
The Catholic University of Leuven has COSIC, focuses on the protection of digital information. COSIC develops advanced cybersecurity solutions to protect data in the cloud and in the Internet of Things (IoT) and to protect the privacy of users.

In addition to their involvement in European projects, they also have studies on differential privacy related to aspects such as e-health, for the protection of patient data, and also in billing, to protect the user's data, for example, any type of payment through the mobile.
PARTICIPATING IN 5 EUROPEAN PROJECTS

- **CONNEXIONS** - InterCOOnected NEXt-Generation Immersive IoT Platform of Crime and Terrorism DetectiON, PredictiON, InvestigatiON, and PreventiON Services
- **PRIPARE** - PReparing Industry to Privacy-by-design by supporting its Application in REsearch
- **PARIS** - PrivAcy pReserving Infrastructure for Surveillance
- **MIDAS** - Meaningful Integration of Data, Analytics and Services
- **FIDELITY** - Fast and trustworthy Identity Delivery and check with ePassports leveraging Traveler privacy

Collaboration with Thales Alenia, University of Málaga and AIT among others, in publications on differential privacy related to aspects such as e-health, for the protection of patient data, and also in billing, to protect the user’s data, for example, any type of payment through of the mobile.

**Participants**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type/Membership</th>
<th>Documents</th>
<th>Authors</th>
<th>Topics</th>
</tr>
</thead>
<tbody>
<tr>
<td>TRAJECT</td>
<td>SMEs</td>
<td>1</td>
<td></td>
<td>computer networks, computer scientists, law</td>
</tr>
<tr>
<td>University of Lyon</td>
<td>University</td>
<td>1</td>
<td></td>
<td>computer networks, computer scientists, law</td>
</tr>
<tr>
<td>University of Namur</td>
<td>University</td>
<td>1</td>
<td></td>
<td>computer networks, computer scientists, law</td>
</tr>
<tr>
<td>AIT Austrian Institute of Technology</td>
<td>Research Lab</td>
<td>1</td>
<td></td>
<td>computer networks, computer scientists, law</td>
</tr>
<tr>
<td>University of Málaga</td>
<td>University</td>
<td>1</td>
<td></td>
<td>computer networks, computer scientists, law</td>
</tr>
<tr>
<td>Thales Alenia</td>
<td>Corporation</td>
<td>1</td>
<td></td>
<td>computer networks, computer scientists, law</td>
</tr>
</tbody>
</table>
This Spanish university, apart from its participation in various European projects, also has several related works on engineering privacy and security by design and the data privacy in smart electrical networks.
Technical University of Madrid – Spain

This Spanish university collaborates with partners such as Atos Spain, Trialog and University of Vigo among others, in several works related to engineering privacy and security by design, and the data privacy in smart electrical networks.

PARTICIPATING IN 2 EUROPEAN PROJECTS

- LASIE - Large Scale Information Exploitation of Forensic Data
- PRIPARE - Preparing Industry to Privacy-by-design by supporting its Application in Research

www.linknovate.com
Technical University of Madrid – Spain
Fraunhofer-Gesellschaft – Germany

PRIPARE - PReparing Industry to Privacy-by-design by supporting its Application in REsearch

FIDELITY - Fast and trustworthy Identity Delivery and check with ePassports leveraging Traveler privacy

SURVEILLE - Surveillance: Ethical Issues, Legal Limitations, and Efficiency

Fraunhofer collaborates with relevant partners across Europe in 3 European projects.
FEED DASHBOARD – “DIFFERENTIAL PRIVACY” ALERT

RECENT REFERENCE

Facebook awards more than 800,000 In Secure the Internet grants

News Article | Site: research.facebook.com/ | Date: August 9, 2018

Michigan State University

Princeton University

Cardiff University

Max Planck Institute for Software Systems

New York University

University of California

Black Hat S.L.

The City College

University of California London

Northwestern University

Cornell University

Facebook

Keywords: Click on them and explore a new topic in our discovery engine facebook, privacy, secure, university, research, grants, user, internet, 80000

Abstract:

Stephen Magill of Galois Inc. was all grins as his name was called to approach the stage and accept his award for verification tools for C++ crytophographic libraries. Alex Stamos, Facebook’s CISO, and I offered the Secure the Internet Grants award with a $100,000 grant to pursue the project.

Magill was one of the 10 winners of our Secure the Internet Grants program, which awarded more than $600,000. Last year during the Black Hat USA conference keynote, we announced that we would fund up to $1 million toward defense-based security research in 2018. We will be awarding another $100,000 through the Internet Defense Prize later this month at the USENIX Security Symposium, as we have done since 2014.
# Linknovate’s FEED insights

## SaTC: CORE: Medium: Collaborative: Rethinking Access Pattern Privacy: From Theory to Practice

**Grant Information:**
- **Agency:** NSF
- **Branch:** Standard Grant
- **Phase:** Secure & Trustworthy Cyberspace
- **Award Amount:** $249,990
- **Date:** 2018-09-01

**Keywords:** Click on them and explore a new topic in our discovery engine
- postdoctoral researchers,
- foundations intellectual merit, notions, practical performance, algorithms, privacy, project rethinks, differentially oblivious algorithms, broader impacts review criteria, cloud outsourcing, access patterns, database scenarios, past techniques, considerable performance overhead, differential privacy analog, secret inputs, graduate students, data structures, privacy notions impact, access pattern privacy, program oblivious, upper bounds, access patterns leak, performance, privacy-preserving algorithms, overhead, remote server, program accesses data stored, project develops open-source libraries, project conceives, high school, data, relaxed notions, leak information, notion called differential obliviousness, project establishes theoretical understanding.

**Abstract:**
When a program accesses data stored in memory, disk, or on a remote server, its access patterns can leak information about the secret inputs and data. There has been decades of work that investigated how to make a program oblivious, such that its access patterns leak nothing about the secret inputs or data. Past techniques, however, incur a considerable performance overhead. This project conceives and investigates new relaxed notions of access pattern privacy, and discovers new algorithms that achieve such notions of privacy with little to no overhead. The project includes training of Ph.D. students and postdoctoral researchers, and mentoring activities focused on high school, undergraduate, and graduate students.

---

### GRANT RELATED

**Dialogflow** is a conversational UX platform enabling brand unique, natural language interactions for devices, applications, and services.

The company raised $8.6M of funds on before been aquired by Google on September 2016.
Your technology search in one place.

Follow us: @linknovate

manuel@linknovate.com