NGI

Partnership for innovative technological solutions to ensure privacy & enhance trust for the human-centric Internet

Webinar, 10 September 2021

NGI TRUST

Webinar – Agenda

Timing	Topic
10:00 – 10:10	Welcome *Jean-Luc Dorel, DG Connect, European Commission*
10:10 – 10:20	Introduction *Alasdair Reid, NGI Trust coordinator, EFIS Centre*
10:20 – 11:35	NGI Trust Funded projects results *NGI Trust Project managers*
11:35 – 11:55	Round table discussion and exchange - Q&A *All*
11:55 – 12:00	Wrap-up and close

NGI TRUST

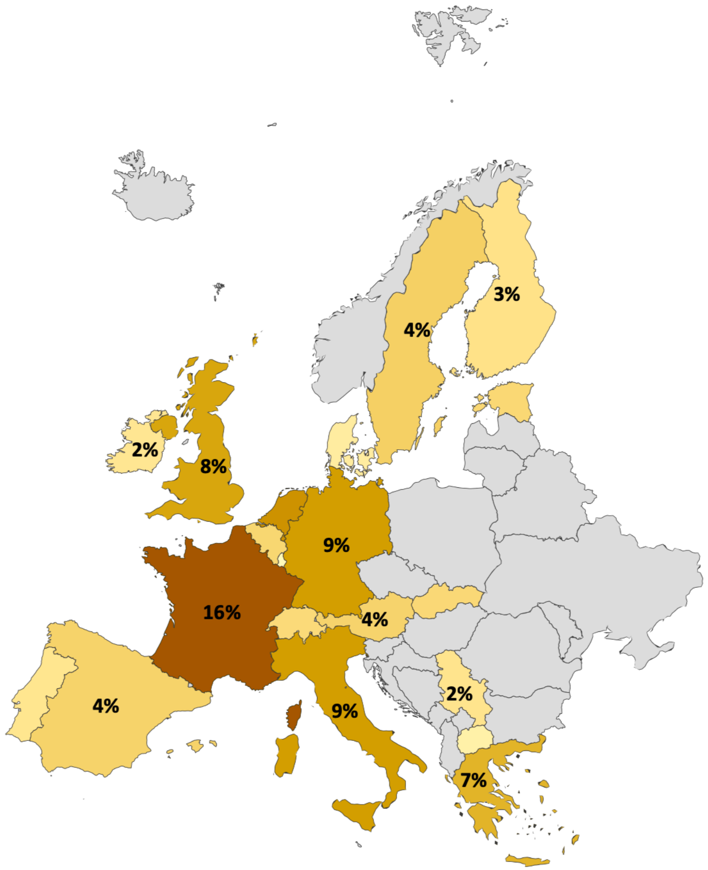
NGI TRUST in a snapshot

Jean-Luc Dorel, DG Connect & Alasdair Reid, EFIS Centre

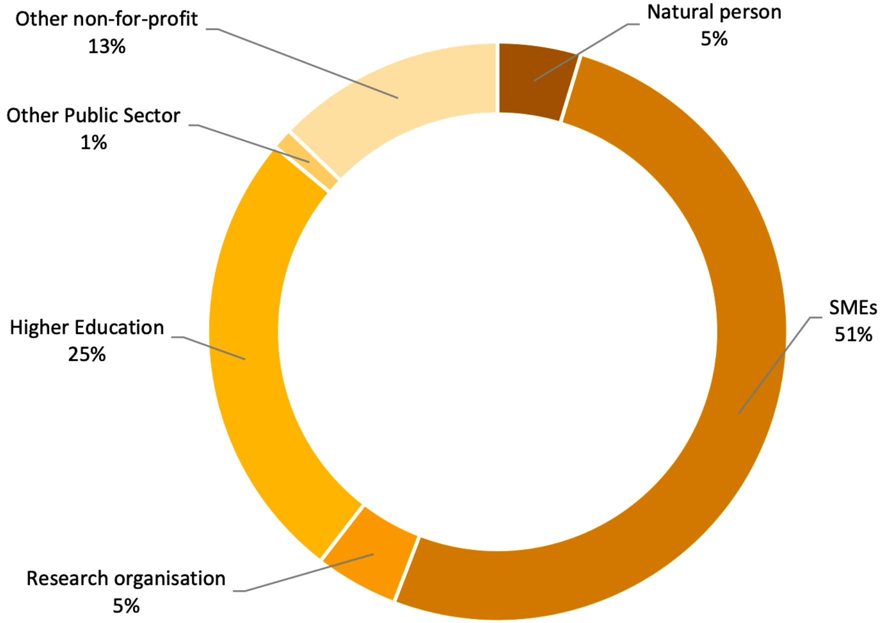
Key facts & figures

- 3 open calls :
  - 300 applications;
  - 448 applicants;
  - 36 countries.
- 3rd party funding: €5.6m:
  - 57 funded projects;
  - 84 funded third parties;
  - 20 countries.

Funding per Country (All Open Calls)



Type of Applicant Organisation



NGI TRUST

NGI TRUST Objectives & Partners

Jean-Luc Dorel, DG Connect & Alasdair Reid, EFIS Centre

Reinforce, structure and develop the **community** of researchers, innovators and technology developers in the field of privacy and trust enhancing technologies

Build on the **state of the art in privacy and trust enhancing** technologies by focusing support for third-party projects in a limited number of priority topics

Improve **user trust and acceptance of emerging technologies** by focusing on applications and solutions that develop a more open, robust and dependable Internet and strengthen Internet Governance

Foster the **exploitation and commercialisation** of the results of selected third-party projects through a tailored process of coaching and mentoring

EFIS

Fraunhofer
IAO

GÉANT
Networks • Services • People

tecnalia
Inspiring Business

ebn
innovation network

kantara™
INITIATIVE EUROPE

NGI TRUST

NGI TRUST

57 PROJECTS FUNDED
12 THEMATIC AREAS

- BEYOND PASSWORDS
- BETTER PRIVACY
- SAFER BROWSING
- USER CONTROL
- IMPACT OF AI
- HUMAN-CENTRIC INTERNET
- STRONGER TOOLS
- EFFECTIVE IDENTITY
- PERSONAL DATA MANAGEMENT
- DATA ETHICS
- SECURING THE INTERNET OF THINGS
- ADVANCING IDENTITY

NGI TRUST Funded projects results

Areas: Securing Internet of Things / Advancing Identity

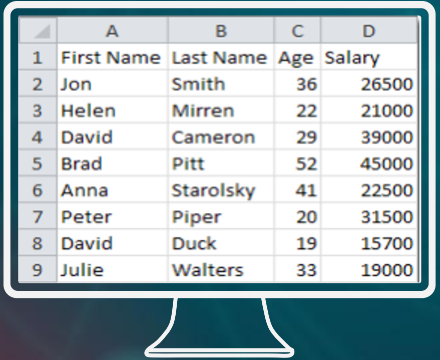
Project	Third party
AnonymAI	CELI, ICT Legal Consulting
IoTrust	Odin Solutions, Digital Worx
TOTEM	Feron Technologies, ntop
PRIMA	Cognitive Innovations
PY/Protect Yourself – PY 2.0	Panga, MyDataBall

AnonymAI

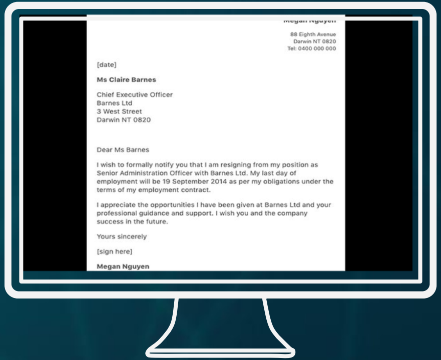
Legally Compliant Anonymization

H-FARM Innovation

What is AnonymAI?



	A	B	C	D
1	First Name	Last Name	Age	Salary
2	Jon	Smith	36	26500
3	Helen	Mirren	22	21000
4	David	Cameron	29	39000
5	Brad	Pitt	52	45000
6	Anna	Starolsky	41	22500
7	Peter	Piper	20	31500
8	David	Duck	19	15700
9	Julie	Walters	33	19000



Megan Nguyen

88 Eighth Avenue
Darwin NT 0820
Tel: 0400 000 000

[date]

Ms Claire Barnes

Chief Executive Officer
Barnes Ltd
3 West Street
Darwin NT 0820

Dear Ms Barnes

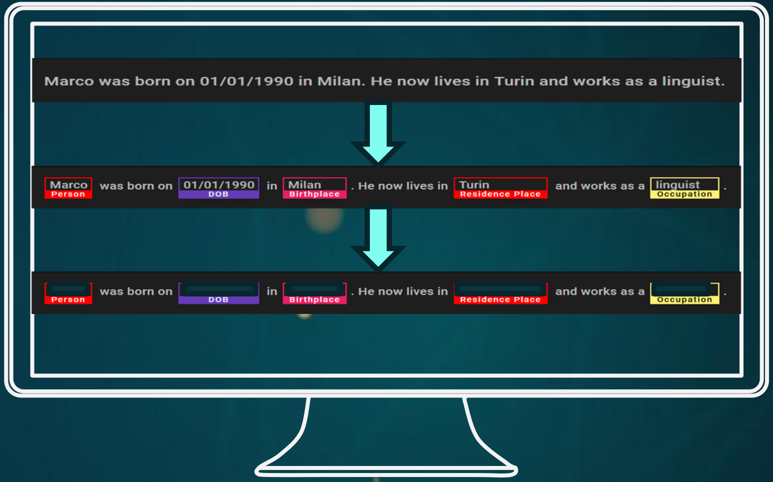
I wish to formally notify you that I am resigning from my position as Senior Administration Officer with Barnes Ltd. My last day of employment will be 19 September 2014 as per my obligations under the terms of my employment contract.

I appreciate the opportunities I have been given at Barnes Ltd and your professional guidance and support. I wish you and the company success in the future.

Yours sincerely

[sign here]

Megan Nguyen



Marco was born on 01/01/1990 in Milan. He now lives in Turin and works as a linguist.

Marco Person was born on 01/01/1990 DOB in Milan Birthplace . He now lives in Turin Residence Place and works as a linguist Occupation .

[redacted] Person was born on [redacted] DOB in [redacted] Birthplace . He now lives in [redacted] Residence Place and works as a [redacted] Occupation .

Direct identifiers

- Name
- Surname
- Email address
- ...

National Identifiers

- Codice fiscale
- ID number
- Passport number
- ...

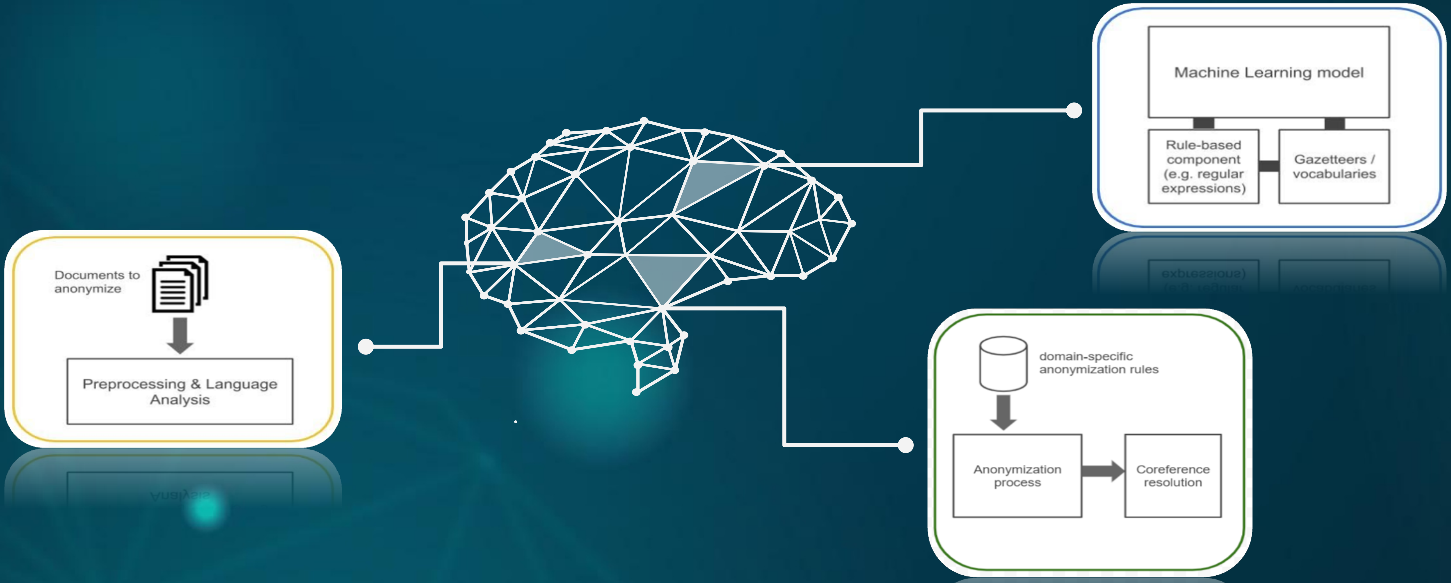
Indirect identifiers

- Civil status
- Nationality
- Age
- ...

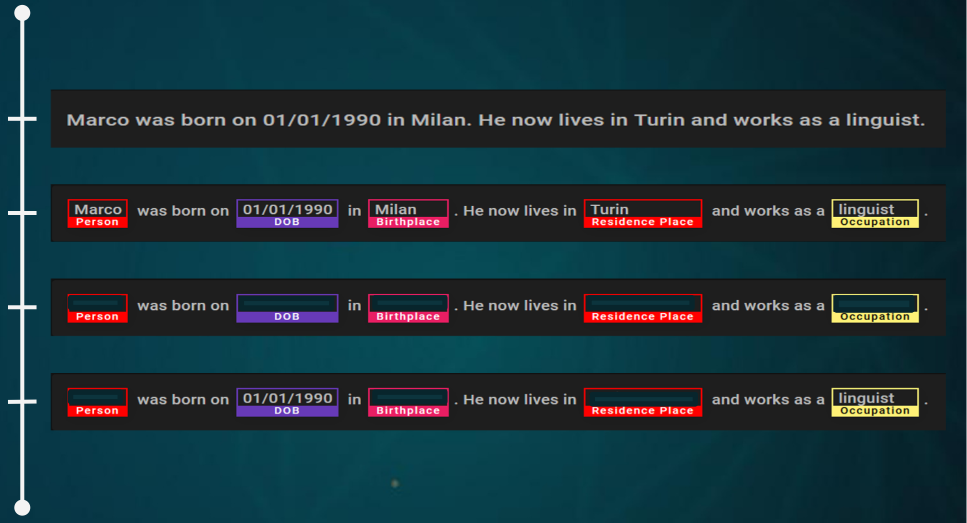
Special Categories

- Sexual orientation
- Health related info
- Ethnic origin
- ...

How does AnonymAI work?



Documents to anonymize
Preprocessing & Language Analysis
Machine Learning model
Rule-based component (e.g. regular expressions)
Gazetteers / vocabularies
domain-specific anonymization rules
Anonymization process
Coreference resolution

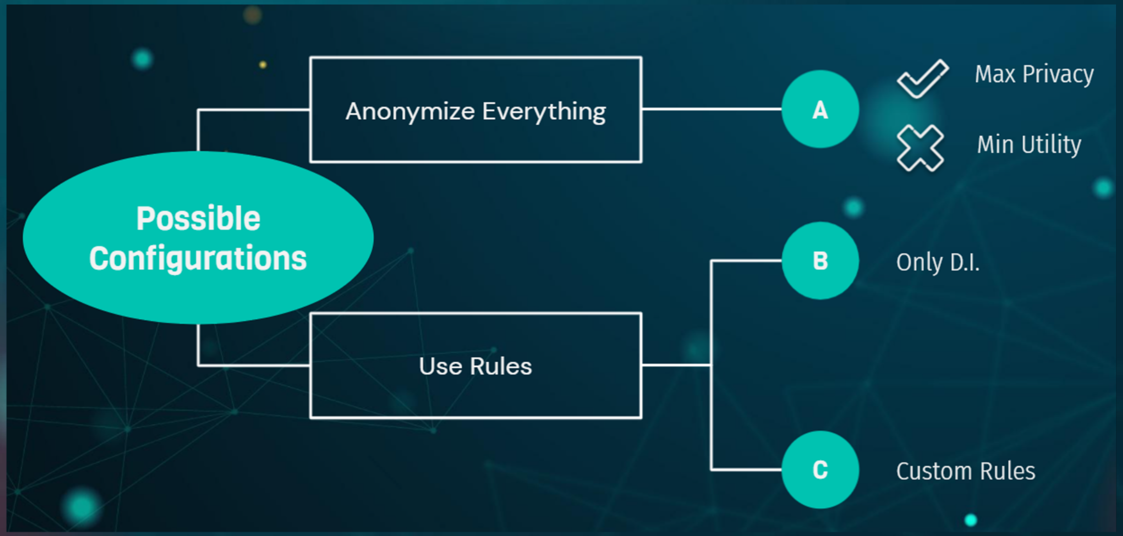


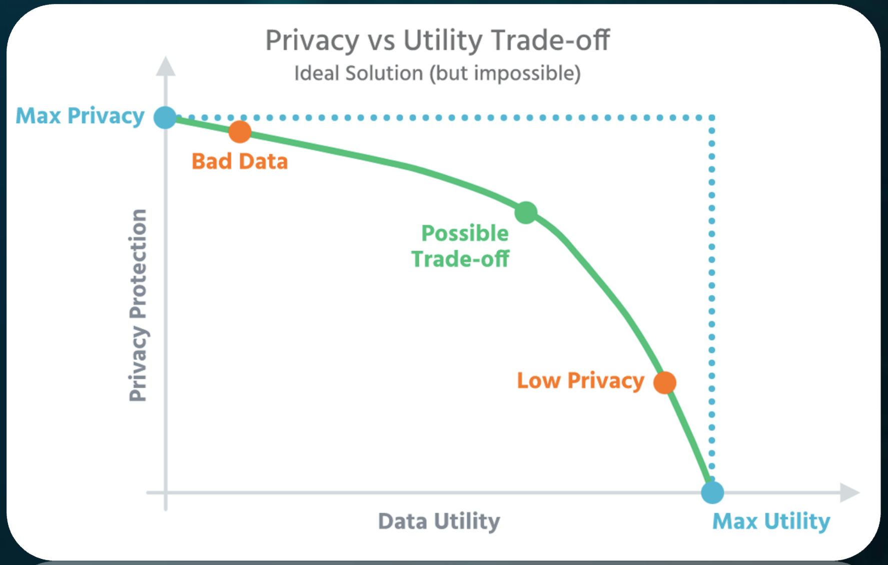
Marco was born on 01/01/1990 in Milan. He now lives in Turin and works as a linguist.

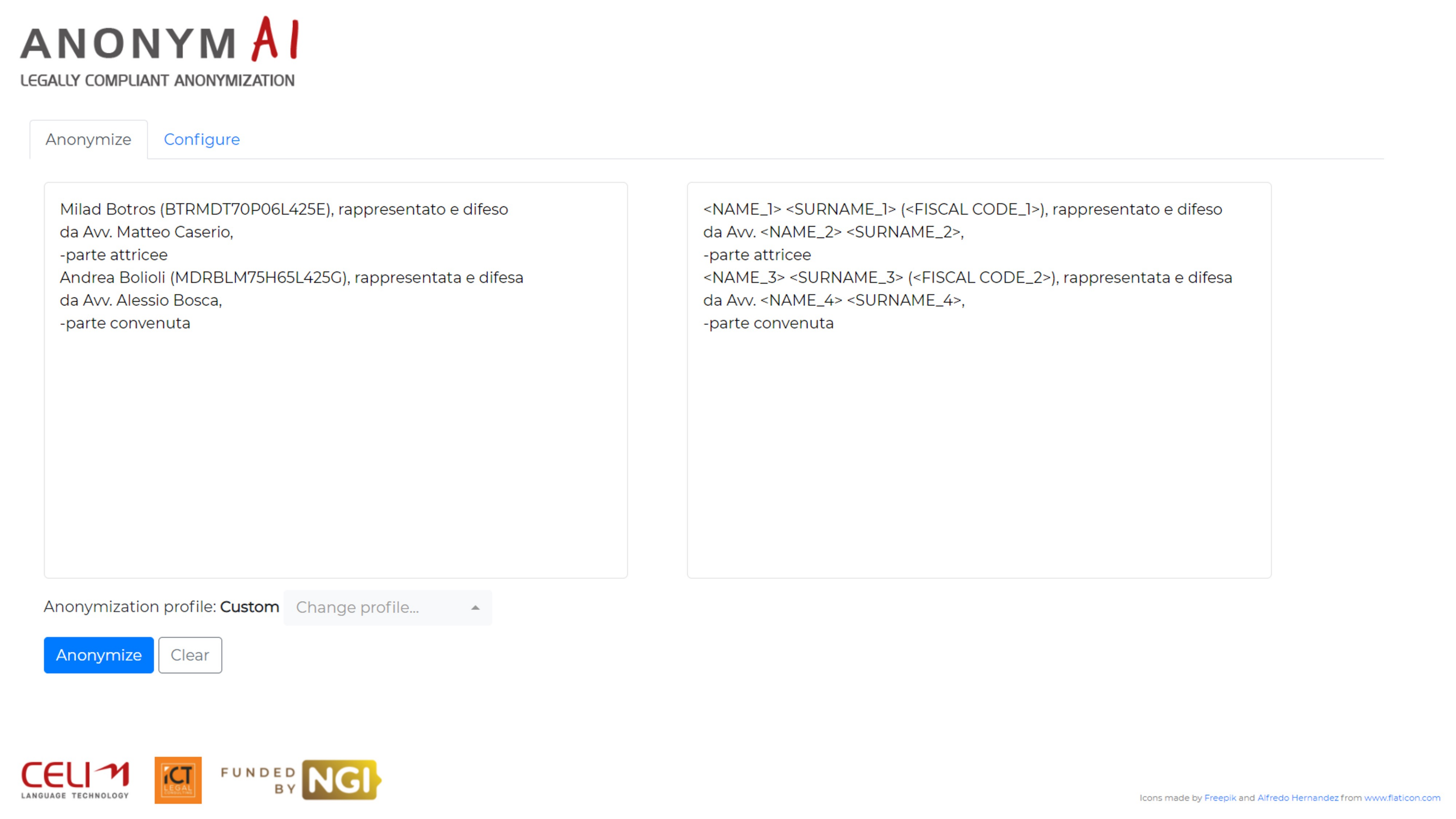
Marco Person was born on 01/01/1990 DOB in Milan Birthplace. He now lives in Turin Residence Place and works as a linguist Occupation.

[redacted] Person was born on [redacted] DOB in [redacted] Birthplace. He now lives in [redacted] Residence Place and works as a [redacted] Occupation.

[redacted] Person was born on 01/01/1990 DOB in [redacted] Birthplace. He now lives in [redacted] Residence Place and works as a linguist Occupation.





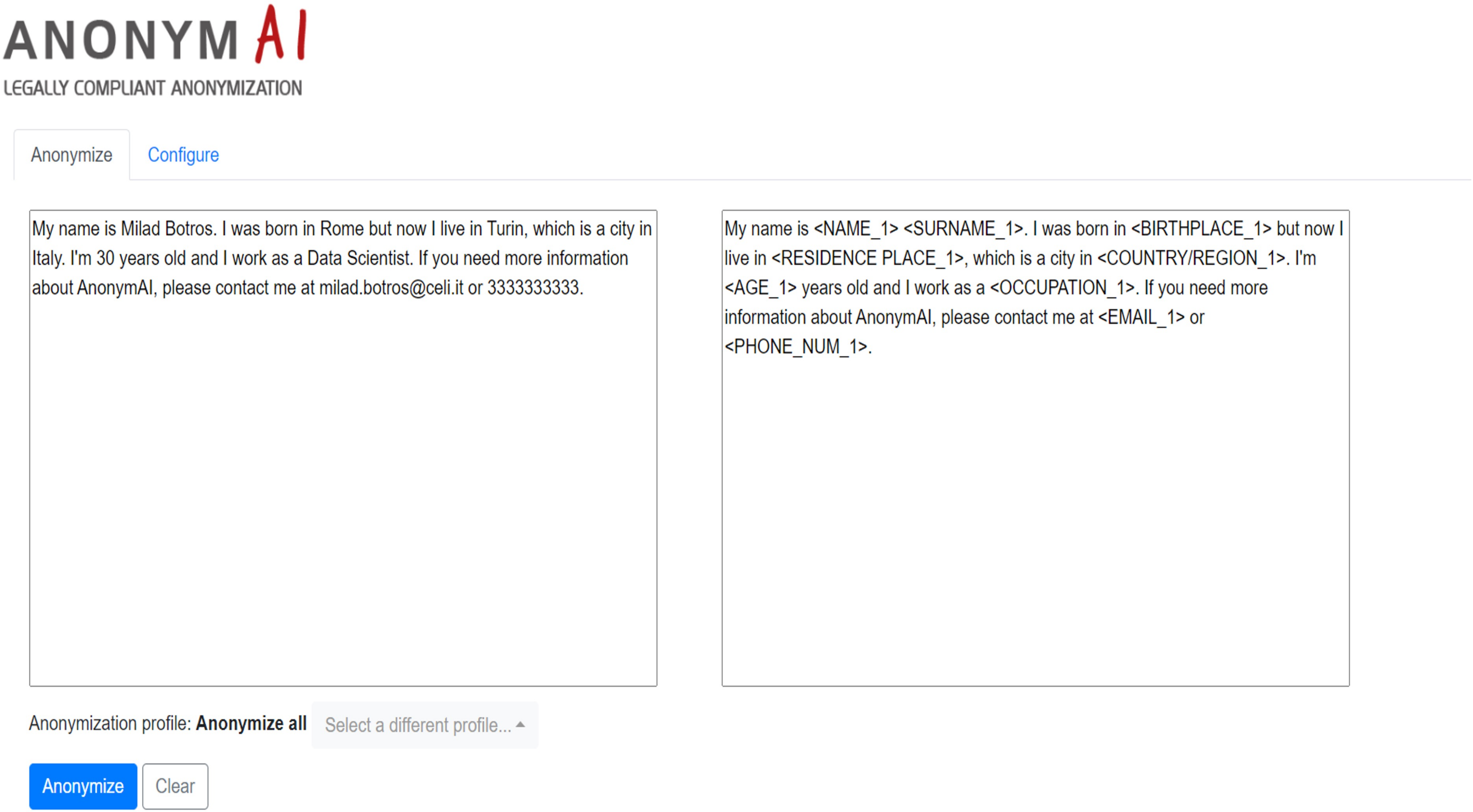


Milad Botros (BTRMDT70P06L425E), rappresentato e difeso
da Avv. Matteo Caserio,
-parte attricee
Andrea Bolioli (MDRBLM75H65L425G), rappresentata e difesa
da Avv. Alessio Bosca,
-parte convenuta

<NAME_1> <SURNAME_1> (<FISCAL CODE_1>), rappresentato e difeso
da Avv. <NAME_2> <SURNAME_2>,
-parte attricee
<NAME_3> <SURNAME_3> (<FISCAL CODE_2>), rappresentata e difesa
da Avv. <NAME_4> <SURNAME_4>,
-parte convenuta

Anonymization profile: **Custom**

Icons made by Freepik and Alfredo Hernandez from www.flaticon.com



ANONYM AI
LEGALLY COMPLIANT ANONYMIZATION
Anonymize
Configure
Select a different profile...
Anonymize
Clear

My name is Milad Botros. I was born in Rome but now I live in Turin, which is a city in Italy. I'm 30 years old and I work as a Data Scientist. If you need more information about AnonymAI, please contact me at milad.botros@celi.it or 3333333333.

My name is <NAME_1> <SURNAME_1>. I was born in <BIRTHPLACE_1> but now I live in <RESIDENCE PLACE_1>, which is a city in <COUNTRY/REGION_1>. I'm <AGE_1> years old and I work as a <OCCUPATION_1>. If you need more information about AnonymAI, please contact me at <EMAIL_1> or <PHONE_NUM_1>.

Anonymization profile: **Anonymize all**

Rafael Marin Perez – ODINS

Mirko Ross - DW

Odin Solutions SL (ODINS) - Spain	OdinS
Digital Worx GmbH (DW) - Germany	digital worx

Objectives & Contributions

- **Main Objective:** a **trustworthy solution to setup and maintain IoT networks** based on the development of *novel technologies (Bootstrapping, Peer-to-Peer and Distributed Ledger)* in order to provide secure initialization of IoT devices, vulnerabilities monitoring and software patching/reprogramming.

- **[O1]** To increase the user trust and application of secure IoT networks in worldwide sectors like Smart Cities, Industry 4.0, etc.
- **[O2]** To achieve trustworthy IoT networks and keep decentralized Internet infrastructure.
- **[O3]** To validate the IoTrust minimum viable product (MVP) using laboratory testbed and real-world pilots.
- **[O4]** To perform dissemination activities and joint exploitation plan.

OdinS

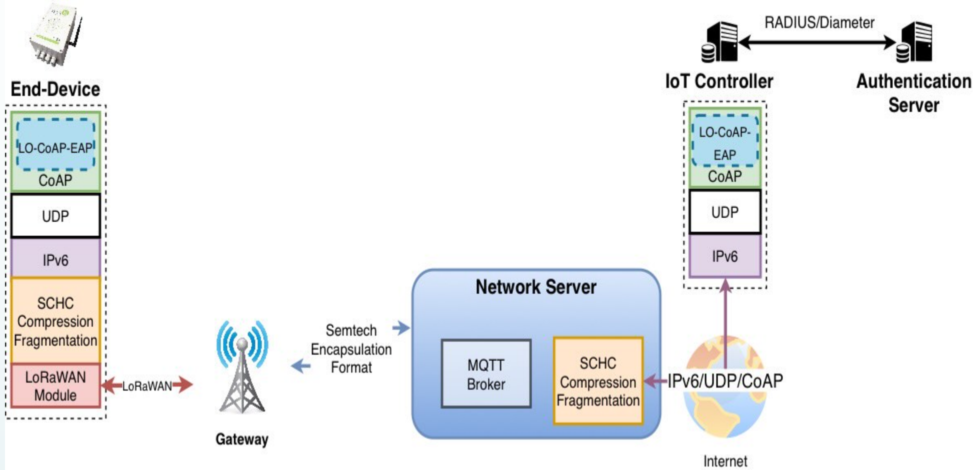
digital worx

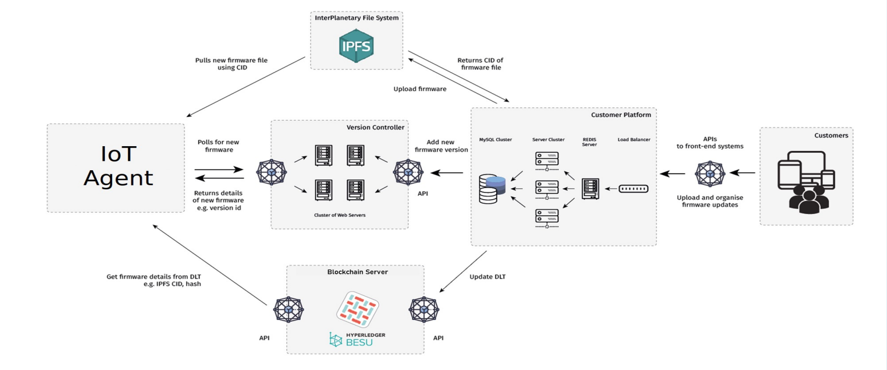
Results & Deliverables

1. IoTrust Solution based on Novel Standards/Technologies
   1. Bootstrapping: SCHC, COAP-EAP, AAA
   2. Firmware Update Over The Air: Blockchain, IPFS
   3. Trust monitoring & anomaly detection: Machine Learning

2. MVP Testbed & Pilot Validation
   - Smart City Pilot (Spain) - ODINS
   - Industry 4.0 Pilot (Germany) - DW

3. Dissemination and Communication
   - Smart Agrifood Summit 2020
   - Building of Internet of Trust. Feb 2021,
   - Paris Space Week. 10 March 2021
   - Scientific Journal, JCR IF 3.367 Q2LPWAN technologies in the 5G ecosystem: A survey on security challenges and solutions
   - Conference paper IEEE International Conference on Smart Internet of Things (SmartIoT 2021)




InterPlanetary File System
IPFS
Pulls new firmware file using CID
Returns CID of firmware file
Upload firmware
IoT Agent
Polls for new firmware
Returns details of new firmware e.g. version id
Version Controller
Cluster of Web Servers
API
Add new firmware version
Customer Platform
MySQL Cluster
Server Cluster
REDIS Server
Load Balancer
APIs to front-end systems
Upload and organise firmware updates
Customers
Get firmware details from DLT e.g. IPFS CID, hash
Update DLT
Blockchain Server
API
HYPERLEDGER BESU
API

Next-Steps

- Incorporate new open standards like IETF OSCORE for efficient data exchange protection.
- International Events
  - Web Summit — November 2021
  - LogiMAT — March 2022
- Exploitation Plan

SHOWCASE INDUSTRIAL DEMOS

FOLLOW AND REACT TO MARKET NEEDS

INTEGRATION WITH OPEN-SOURCE PROJECTS

OdinS

digital worx

NGI

TOTEM

Trust-Enhancing TechnOlogies CommodiTization for IncrEasing Security Awareness in Connected HoMes

FERON TECHNOLOGIES P.C. & ntop

8th Results Webinar, September, 10th, 2021

Antonis Gotsis (FERON) & Luca Deri (ntop)

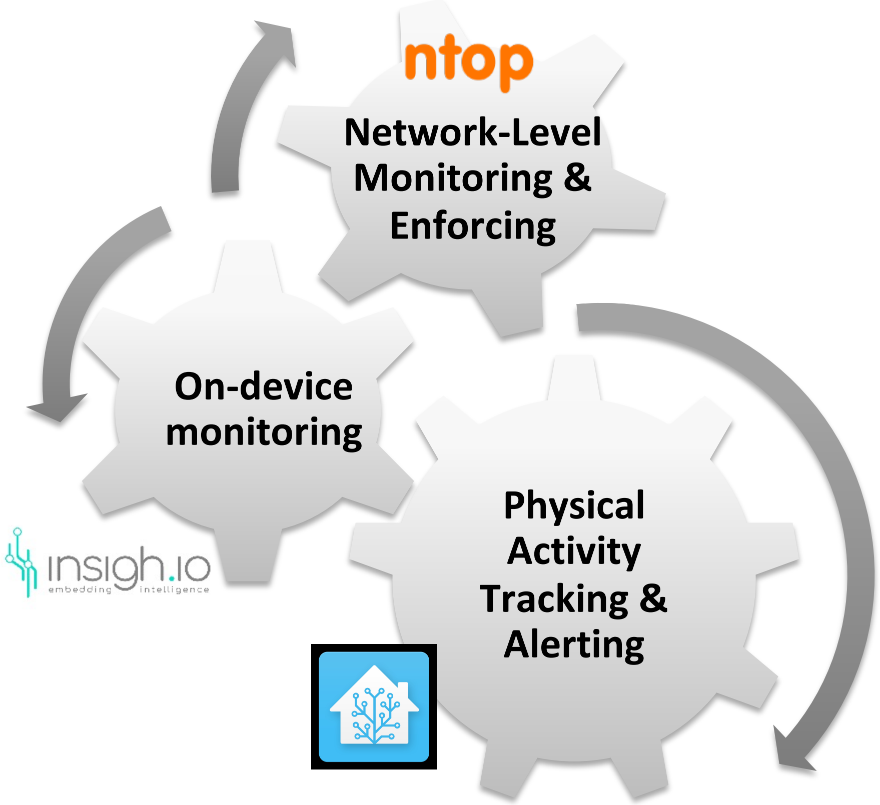
antonis.gotsis@feron-tech.com & deri@ntop.org

Project Vision & Objectives

Value Proposition: In a connected home with many heterogeneous end-points, we want to *simplify, automate and eventually make accessible to tech and non-expert users a set of tools for proper control of end-points and early identification of potential malicious operation.*

Objectives

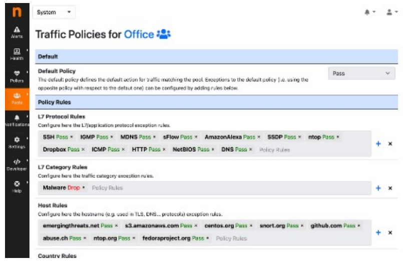
- *Empower the home network with network monitoring and enforcing capabilities*
- *Augment the end-points with advanced monitoring capabilities*
- *Complement the monitoring capabilities with physical activity tracking & alerting*
- *Develop an open and fully configurable connected home testing environment*
- *Bundle the TOTEM tools Into a low-cost general-purpose hardware board*



ntop
Network-Level Monitoring & Enforcing
On-device monitoring
insigh.io embedding intelligence
Physical Activity Tracking & Alerting

Project Key Results

Outcome Types
☑ Extensions to existing product
☑ End-User Tools
☑ Demonstration
☑ Community Contributions


System

Traffic Policies for Office

Default

Default Policy
The default policy defines the default action for traffic matching the pool. Exceptions to the default policy (i.e. using the opposite policy with respect to the default one) can be configured by adding rules below.
Pass

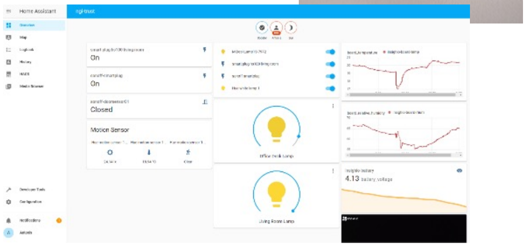
Policy Rules

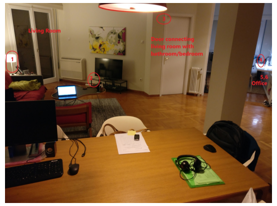
L7 Protocol Rules
Configure here the L7/application protocol exception rules.
SSH Pass × IGMP Pass × MDNS Pass × sFlow Pass × AmazonAlexa Pass × SSDP Pass × ntop Pass × Dropbox Pass × ICMP Pass × HTTP Pass × NetBIOS Pass × DNS Pass × Policy Rules

L7 Category Rules
Configure here the traffic category exception rules.
Malware Drop × Policy Rules

Host Rules
Configure here the hostname (e.g. used in TLS, DNS... protocols) exception rules.
emergingthreats.net Pass × s3.amazonaws.com Pass × centos.org Pass × snort.org Pass × github.com Pass × abuse.ch Pass × ntop.org Pass × fedoraproject.org Pass × Policy Rules

Country Rules





Key Result	Description	Lead Partner	Open-Source Repository
I	A collection of software stacks for transparent home network monitoring and policy enforcing extending ntop's ntopng, nProbe and nDPI tools to the IoT use-case.	ntop	https://github.com/ntop/
II	Software library extending FERON's partner IoT codebase, used for embedding cybersecurity-aware device monitoring capabilities in ESP32-based IoT end-points	FERON	https://github.com/insighio/
III	Software Plug-in to Home-Assistant for use in connected home devices physical activity monitoring, characterization and end-user alerting	FERON	https://github.com/feron-tech/
IV	TOTEM testbed for testing project technologies and tools in real-world conditions with the use of COTS connected home devices	Both	-

4 webinars + 4 scientific publications

Project Impact & Next Steps

✓ **NGI & Community**

- Trust-enhancing technologies as an NGI strategic pillar for human-centric internet
- IoT trust tools (SW, HW, platforms) for increasing trust and cybersecurity awareness in Connected Homes
- Used by technology domain experts (open-source & documentation)
- Or by the general public (automated & user-friendly)

✓ **FERON Partner: Full-stack IoT**

- **Address new markets, such as Smart Homes & IoT Cybersecurity**

✓ **Ntop: High-quality networking software**

- **Improve support and focus for IoT and Smart Home Applications**

✓ **Joint Outcome for Further Exploration**

- **"TOTEM-in-a-box“**: A **hardware** & **software** bundle of home **management** and **monitoring** tools, both in-house and customized 3rd party ones, in a **commodity low-cost** computing **board**

List of Publicly Available Output

Open-Source Contributions

1. https://github.com/ntop/ntopng/
2. https://github.com/ntop/nProbe
3. https://github.com/ntop/nDPI
4. https://github.com/insighio/insighioNode
5. https://github.com/feron-tech/ngitotem-sensor-alarming
6. https://github.com/feron-tech/ngitotem-home-assistant

Videos of Presentations, Webinars, Tutorials

1. ntop mini conference 2020: https://youtu.be/TwdRbboERB0
2. FOSDEM 2021: https://youtu.be/CV6-HAQPv3M
3. ntop Webinar on pfSense/OPNsense 2021 https://youtu.be/_FCx6Y1ZD1o
4. nProbe IPS – Inline Traffic Policer https://youtu.be/0Pn2kS4NvFY
5. Traffic Visibility and Policing of Smart Home: https://youtu.be/de9M-Od48

PRIMA – PRIvacy preserving IoT data analysis using federated MAchine learning protocol

Cogninn

Cognitive Innovations Private Company

Kifisias Av. 125-127, 11524

Athens, Greece

http://cogninn.com/

Challenge addressed

1. **Future Internet** will be able to integrate the ML knowledge from the surrounding environment.
2. **Distributed ML** will be able to train models both to the IoT devices and edge servers.
3. **PRIMA protocol** will specify all the required distributed rules among the IoT and edge computing infrastructures to train ML in a distributed fashion as provided by federated learning.

Results expected

- A federated learning specification for IoT devices, where the edge intelligence with the IoT are integrated in an efficient manner.
- Constrained and non-constrained devices will be considered for the protocol specification and implementation.
- PRIMA will target advanced IoT use cases such as Augmented Reality (AR) services in future smart cities, where the users will be able to integrate knowledge from the surrounding city environment.
- PRIMA will be tested to a Fed4Fire testbed and evaluated in terms of federated training and communication performance.

PYGUARD

PY & PY 2.0

Protect Yourself

NGI TRUST

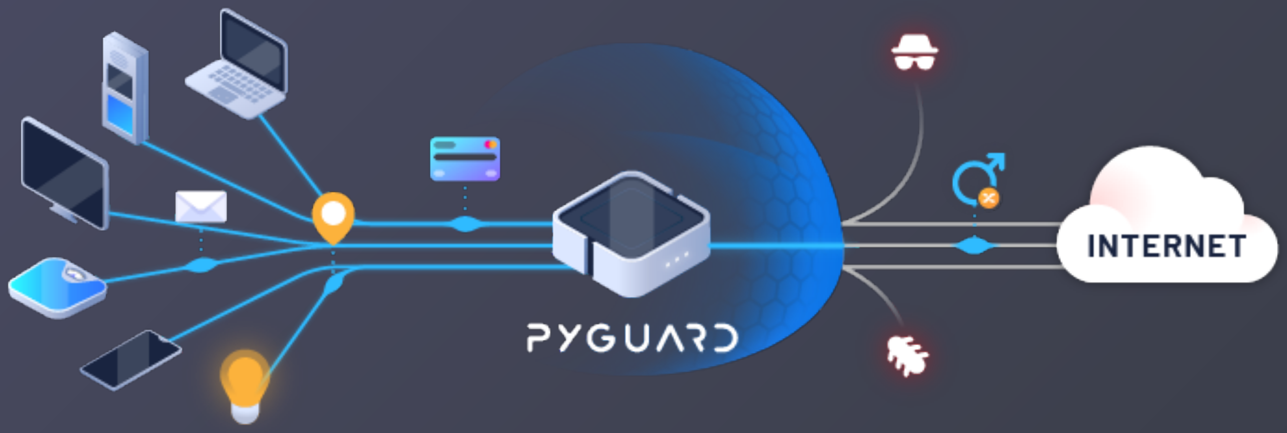
mydataball

Panga

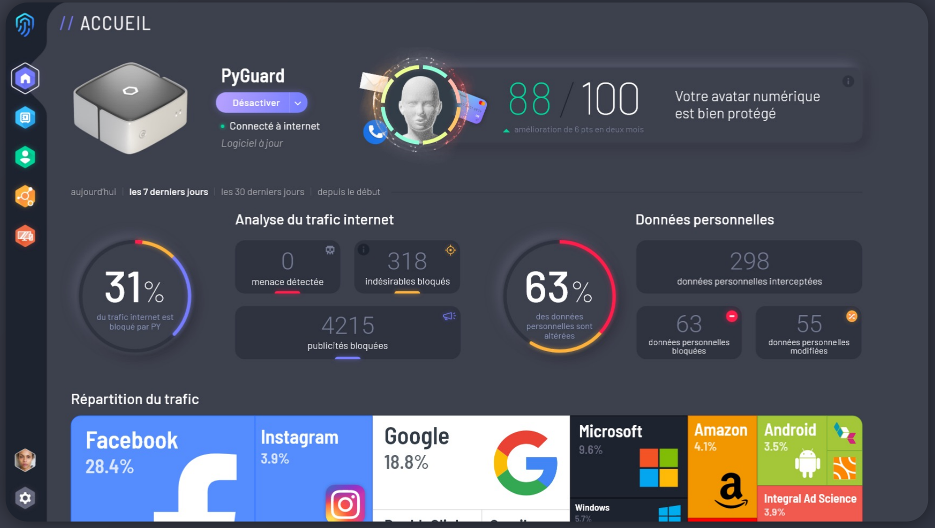
Personal data protection project carried by french startup PANGA

Objectives & Contributions

How can we protect the average user's privacy and personal data stemming from their connected devices, with minimal changes in their habits, while respecting their data sovereignty ?



PyGuard filters unwanted connections and personal data stemming from connected devices while raising user awareness about privacy



// ACCUEIL

PyGuard

Désactiver

Connecté à internet

Logiciel à jour

88 / 100

amélioration de 6 pts en deux mois

Votre avatar numérique est bien protégé

aujourd'hui | **les 7 derniers jours** | les 30 derniers jours | depuis le début

Analyse du trafic internet

31% du trafic internet est bloqué par PY

0 menace détectée

318 indésirables bloqués

4215 publicités bloquées

Données personnelles

63% des données personnelles sont altérées

298 données personnelles interceptées

63 données personnelles bloquées

55 données personnelles modifiées

Répartition du trafic

Facebook 28.4%

Instagram 3.9%

Google 18.8%

Microsoft 9.6%

Windows 5.7%

Amazon 4.1%

Android 3.5%

Integral Ad Science 3.9%

Main objective :

Industrializing our prototype into a marketable MVP

- Industrializing our PoC & provisioning
- Developing the production chain and distribution channels
- Finding our business model & work on commercialization
- Building trust through standards compliance, tests and certifications

Results

From concept to prototype to MVP

- **Evolution in knowledge of ways to protect individuals' personal data**
- **Algorithms / IP :**
  - Cyberscore
  - Website categorization
  - Personal data categorization
- **2 B2B2C scenarios / business models :**
  - Insurers / ISP distribution (first sales)
  - Integration to our Smart Building gateways
- **An MVP with its production chain :**
  - Edge-computing hardware platform analyzing all network packets in real-time
  - Packaging, inserts, user manual, accessories
  - Software (Web dashboard, web plugin, mobile app (alpha stage))

Web application

PyGuard's UI demonstration

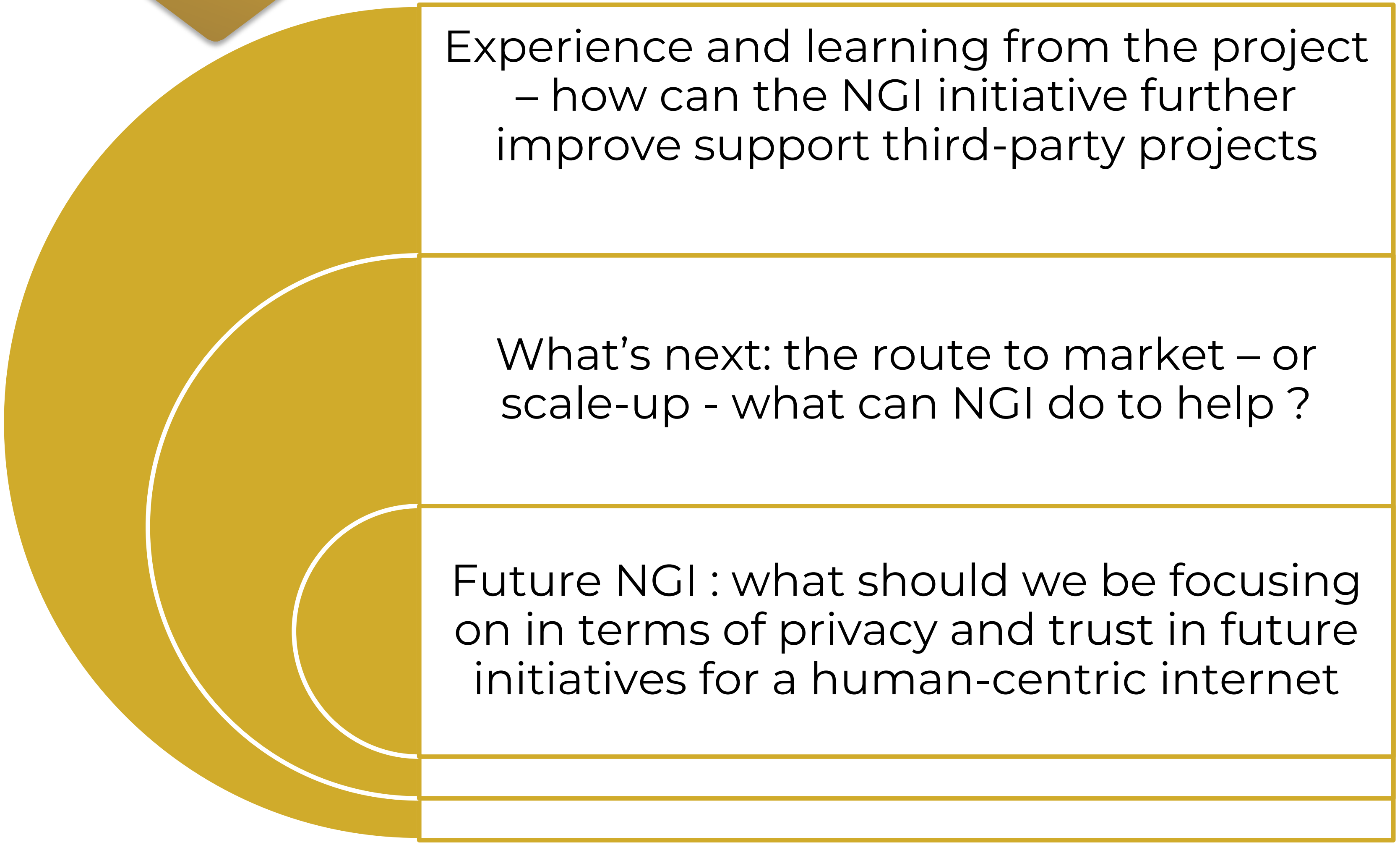
Plugin

Mobile app *(alpha stage)*

Next steps

- **Focus on first sales**
- **Fundraising Q1 2022**
- External certification with trusted third-parties
- Mobile App launch
- Expand functionalities (SSO, parental control...) and IoT support (cameras, sensors, smart TV, health related connected devices)
- Integration / support with decentralized internet projects by making PyGuard a node (SOLID, DAppNode...)

Round table discussion and exchange - Q&A



Experience and learning from the project – how can the NGI initiative further improve support third-party projects

What’s next: the route to market – or scale-up - what can NGI do to help ?

Future NGI : what should we be focusing on in terms of privacy and trust in future initiatives for a human-centric internet

More information/contact us

- Project coordinator : Mr Alasdair Reid @ EFIS Centre - www.efiscentre.eu
- Email : NGI-Trust-support@lists.geant.org
- Twitter: @NgiTrust
- NGI_TRUST wiki : https://wiki.geant.org/display/NGITrust
- NGI.eu website : https://www.ngi.eu/about/

The NGI_TRUST project has received funding from the European Union’s Horizon 2020 Research and Innovation Programme under Grant Agreement No 825618

NGI TRUST