# Data sovereignty: PyGuard protects your privacy online

## Summary

PyGuard is a cybersecurity project that protects individuals from online tracking. In the past decades, Big Tech companies such as GAFAM[1] and BATX[2] have developed business models relying on the sale of our personal data. However, they represent a risk for our privacy, our freedom of choice and free-will, due to targeted ads, news, and sponsored content. Furthermore, phishing and cyberattacks are increasing, while we introduce more and more numerous yet vulnerable connected devices into our homes.

PyGuard is an all-in-one hardware platform with embedded software that protects and manages locally your personal data, credential information and connected devices, even beyond your home. Regaining the sovereignty of our data is a personal, societal, and political issue. Together, let's reclaim our privacy!

## Keywords

Personal data; cybersecurity; privacy; cyberscore; data sovereignty; connected devices; IoT; online tracking; Privacy by Design; GDPR; Digital Avatar.

## Actors involved in the project

- Panga
- MyDataBall
- MAIF Foundation
- Research Institute Xlim
- Computer, Image and Interaction Research Laboratory L3i of the La Rochelle University

[1] *Google Amazon Facebook Apple Microsoft*

[2] *Baidu Alibaba Tencent Xiaomi*

## How it started

PyGuard is a cybersecurity and privacy project that protects individuals from online tracking, developed by Panga since 2015. Patrick Simon, an expert in network and telecommunication for 20 years, is the founder of Panga, a French startup based in La Rochelle by the Atlantic coast. Our primary activity is to develop an edge computing network architecture for Smart Buildings and Smart Cities. From the start, Panga has been promoting decentralized networks, as a way to both reduce the energy consumption of communication architectures, and to ensure the sovereignty of sensitive data.

Followed by a team of now 9 members, all concerned about data privacy, the PyGuard project was soon started, whose goal was to protect personal data stemming from connected devices. The French startup MyDataBall, expert in Artificial Intelligence, as well as academic research laboratories such as the XLIM or the L3i also joined the adventure.

Supported from the start by the *Fondation MAIF*, a foundation of public interest that finances scientific research about risks such as cybersecurity or digital risks, PyGuard was selected by NGI_Trust under the name PY: Protect Yourself, as a 12-months project to be started in September 2019.

## What was the problem?

PyGuard targets a complex issue, which was recently brought to light in the Netflix documentary *The Social Dilemma*. Our connected devices, smartphones and computers generate personal data, which reflect our opinions and lifestyle. Big Techs business models rely on our personal data, to offer the most accurate platforms to broadcast targeted ads and sponsored content. Beyond raising concerns about our freedom of choice and manipulation through dark design patterns or nudges, it also raises privacy and cybersecurity issues, as these data are often being sent to third parties without our knowledge. What seemed yesterday like science-fiction straight out of the Netflix show *Black Mirror* is now reality, through scandals such as *Cambridge Analytica*.

We want to give average users a way to reclaim their privacy in the face of GAFAM's hegemony and stop the leak of their personal data at the source. So, we needed to imagine a solution that would both increase the security of connected devices without requiring technical knowledge, as well as filter personal data, ads and unwanted connections to prevent online tracking.

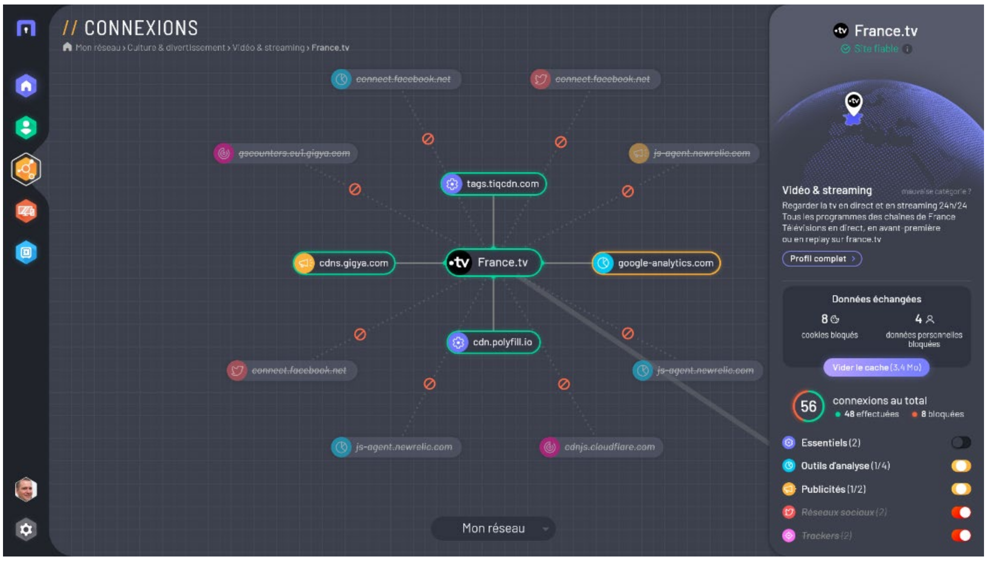
All of this, without compromising user's sovereignty over their data by forcing them to place their faith in the virtue of a private company, which is why we chose to provide users with their own server, located in their home and inaccessible from the outside.

## The PyGuard Solution

PyGuard's first objectives were to develop a prototype acting as a central checkpoint for all connected devices. The hardware and software solution should raise users' awareness about privacy and about the security of their data, as well as protect citizens from third-party connections and unwanted data flows that happen automatically when a device is connected to the internet. Through a user-friendly interface, the system would graphically

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 825618

provide an overview of all network activities and personal data interceptions and allow users to easily set their own security and privacy settings.



Regarder la tv en direct et en streaming 24h/24
Tous les programmes des chaînes de France Télévisions en direct, en avant-première ou en replay sur france.tv

*Figure 1. PyGuard Interface showing overview of all network activities.*

Being an all-in-one solution, PyGuard includes existing technologies to protect and anonymize oneself on the internet, such as a VPN, an embedded firewall or an upstream antivirus that blocks threats before they even reach devices. But it also relies on new edge technologies that were specifically developed, such as a proxy capable of identifying, modifying or blocking personal data in requests; a neural network categorizing connections in order for PyGuard to be smart and autonomous in its blocking choices; or complex algorithms to define the trustworthiness of a connection.

All that complexity is hidden from the users by the metaphor of Digital Personal Avatars: profiles representing how we are perceived on the internet, based on our personal data. PyGuard adapts the level of anonymity of users for each website.

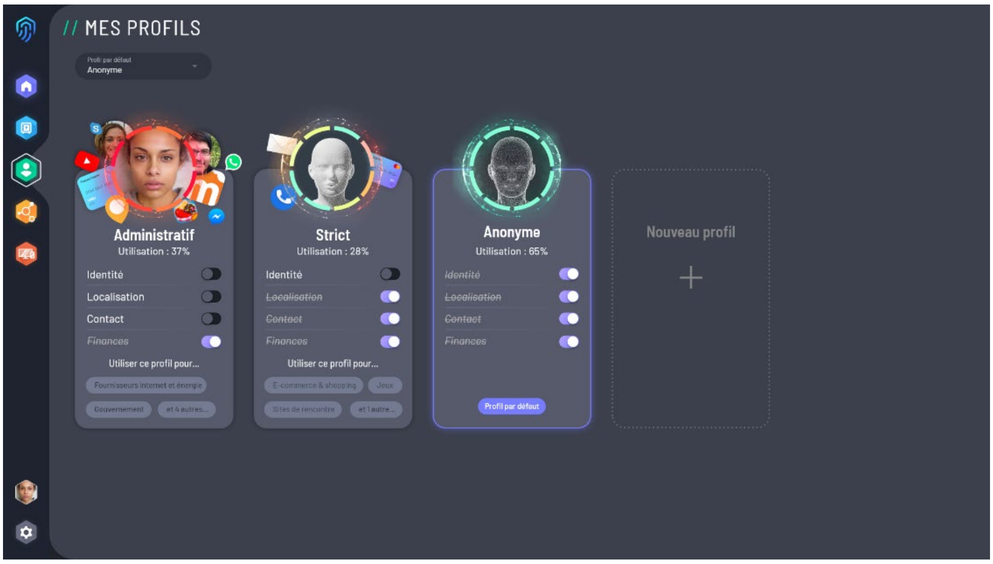


*Figure 2. Digital Personal Avatars*

Our project contributes to a human-centric internet because it empowers users without technical knowledge to reclaim their privacy. We relocate the data near the user, following the principles of the *SOLID project* from Tim Berners-Lee.

To us, privacy means anything personal that you could want to keep private, from political or religious opinions, online behaviours, movies you like, conversations with friends, to your very name. In western democracies, we tend to take privacy as a secondary concern, thinking what happens in more authoritarian countries can't happen to ours, forgetting History, and believing that privacy only matters "if we have something to hide". On the contrary, we believe it's a fundamental right that should be carefully protected.

We think PyGuard distinguishes itself from alternative data security solutions because it is convenient: it offers high level of protection autonomously, without impeding usage. Filtering at the network level rather than the device one also means that users don't have to find a security solution for each of their connected device. Furthermore, PyGuard was designed for non-technical users, which usually is an exception among most cybersecurity solutions.

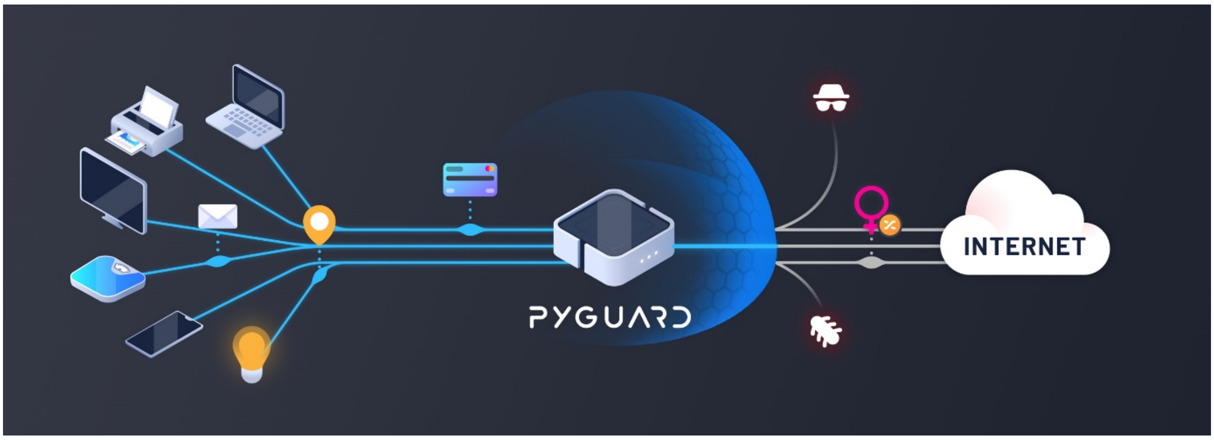


*Figure 3. The PyGuard Solution*

## Where do we stand?

Being an ambitious project from the start, we nevertheless managed to reach our goal and deliver a prototype for the NGI project, with the core functionalities we set out. NGI renewed its trust in our project and 2021 will be the year for productization and commercialization for PyGuard.

For now, three prototypes are available for demonstration in the showroom of the *Fondation MAIF* and on the *MAIF Numerique Tour*, from whom we are getting our first "production" user feedback. Currently, we have only demonstrated PyGuard at a smaller scale, but we are quite excited about the tester's reactions. There is a "wow, I wasn't expecting that" effect upon discovering all the hidden connections happening without our knowledge. We provide users

*Figure 4. PyGuard Prototype*

with statistics, about which countries they connect to in real-time, which companies generate the most connections, which personal data was retrieved, and this highlights interesting results. As one of our most compelling examples, we discovered that one of the biggest French retail websites sends Facebook data about all user's queries and about every product page they visit, accompanied with keywords targeting possible related interests.

We think our project is complementary with the rest of the European ecosystem of researchers, innovators, and technology developers, as our goal is to integrate and make available the latest innovations when it comes to privacy, to average users.

## Testimonial

Working with NGI_Trust was a positive opportunity business wise, as it gave the project legitimacy in our funding research and boosted it into its next phase. Being part of the NGI_Trust ecosystem also gave us access to key resources, such as one-on-one coaching and business mentoring. Having coaching sessions is a real benefit to the project development, and we are glad to keep working with Eider Iturbe and Robin Wilton this year, since they provided us with varied advices and insights, from suggestions on functionalities to priorities when it comes to project management. They also brought to our knowledge relevant European resources, standards, and projects that we wouldn't have heard of without them.

We initially applied to NGI_Trust because PyGuard seemed quite relevant to the areas of concern described in the open call. This experience furthered our expectations when it comes to the support NGI_Trust provides to its grantees, and we could only recommend it to other projects.

## Our future plans

We have many ideas for future developments and are quite ambitious about the project, although we are now focusing onto releasing our first commercial product.

Interoperability between all the solutions promoted by NGI_Trust and the European Commission will be the key to building a sustainable alternative to GAFAMs for users and reclaim sovereignty over our data and privacy.

*For more information, visit PyGuard: https://www.pyguard.fr/en*

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 825618