Horizon 2020 Programme
DG CNECT
Next-generation Internet

NGI TRUST

Grant Agreement number: **825618**

Project acronym: **NGI_TRUST**

Project title: **Partnership for innovative technological solutions to ensure privacy and enhance trust for the human-centric Internet**

Type of action: Research and Innovation Actions (RIA)

Deliverable 4.1

Case studies published

Deliverables leader:	**GÉANT**
Authors:	Auke Pals
Due date:	30-09-2021
Actual submission date:	06-10-2021
Dissemination level:	Public

Abstract: This report is part of a project that has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 825618

Document Revision History

Date	Version	Author/Editor/Contributor	Summary of main changes / Status
20-04-2021	0.1	Auke Pals	Creation of document
26-09-2021	0.2	Auke Pals	First draft ready
27-09-2021	0.3	Nicole Harris	Review of first draft
01-10-2021	0.4	Auke Pals	Inserted changes after feedback

Disclaimer

The sole responsibility for the content of this publication lies with the authors. It does not necessarily reflect the opinion of the European Commission. The European Commission is not responsible for any use that may be made of the information contained therein.

Copyright

This document may change without notice.

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

Table of content

List of Figures

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

1 Executive Summary

This deliverable outlines the strategy on the approach to get case studies published for the NGI_Trust projects. It provides details on the main objectives, selection, method of gathering the case studies and the communication channels. The case studies outline the importance and impact of the projects ensuring that research infrastructure managers, policy makers and funders, and other interested stakeholders rapidly become aware of the projects and impact of the NGI_Trust project.

This deliverable includes the main objective indicate, which is inline with the key performance indicators (KPIs) that have been defined in the communication plan and a reflection on how these have been met.

2 Introduction

2.1 Background / Deliverable Description

The objective of NGI_Trust dissemination activities is directly related to the expected impact of the call topic, especially towards building a European ecosystem of researchers, innovation, and technology developers in the field of privacy and trust enhancing technologies. In this context, NGI_Trust recognises that strong outreach is key for successfully promoting the Open Calls. One of the pillars in the outreach strategy is showcasing project outcomes. They will cover real life examples of the activities conducted and results from the NGI_Trust Open Calls.

As described in deliverable 2.2 one of the activities defined in the communications plan is to showcase project outcomes.

Why, What, to Whom, Where, When and How to disseminate project outcomes NGI_Trust in the form of case studies.

Why: According to the communication strategy, promote project outcomes of Open Calls, which attracts new participants in future calls.

What: Written case studies of up to 10 NGI_Trust projects.

To Whom: Future Open Call audience, Researchers, General public.

Where: NGI_Trust website, CONNECT magazine and spread in networks.

When: Month 29, Month 31, Month 33.

How: A case study template has been created by the communication team, with that the NGI_Trust supported projects have created a case study which has been published.

Background

NGI_Trust supports the development of a human-centric Internet through open calls. By creating case studies, the successes of the NGI_Trust projects are shared,

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

and audiences are inspired and will possibly apply for the next round of funding or collaborate with existing projects.

Objectives

The objective is to have formal case studies about funded projects and achievements to meet this deliverable. The KPI set is to have case studies published from 5-10% of the total projects funded. Case Studies are intended to generally showcase projects and do not have a specific intent for the projects (e.g. ongoing funding).

Targets

As outlined in the communication plan, the KPI of the deliverable is to have up to 10 NGI_Trust projects case studies published.

2.2 Relation to other NGI_Trust deliverables

This deliverable *"4.1: Case studies published"* is related to deliverable D2.2: NGI_Trust communication plan. That plan describes several forms of communication activities that contributes the community and projects in their outreach activities. One of these activities is gathering successful case studies from the projects that got funded through the open calls.

3 Work done

In this section the methodology of the work done in order to publish the case studies is described. This leads to the results and current status of the case studies being published.

3.1 Methodology / Networking and collaboration

Template

The coaches informed the communications team that many project staff members were interested in writing a case study but lack expertise. As a result of this observation, the NGI_Trust communications team created a template describing the usefulness of the case study with a set of structured questions. The project staff were then asked to take these questions as a guide and answer them in a running narrative. The template is available in Annex 1.

Selecting projects

Due to the different starting dates of projects, case studies were also published in three phases.

When the projects from the various calls had finished their final reports, the coaches were approached to make suggestions for interesting and potential projects. The coaches made a selection from their portfolio of eligible projects.

The selection criteria were that a maximum of three projects would be selected from each call, as we set a KPI of no more than ten projects in our communication plan.

Approaching projects

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

The project main investigators were contacted and asked whether they were interested in giving their project a wider reach. Several projects were pleased to be selected (Annex 2, email 1).

After receiving confirmation from the project teams, they were sent the template describing how we the case study should be structured and delivered. (Annex 2, email 2).

Support was given to some projects by email with suggestions to make the case study more attractive by adding images or extend the case study to a follow-up project within NGI_trust (e.g. CASPER & CASPER 2.0).

Furthermore, several projects needed more time to complete the case study; this caused some delay in the timeline but did not significantly impact the project to publish the case studies.

Cleaning up the case study

After the NGI_Trust communication team had received the case studies, the team reviewed the case studies for grammar and structure. If any questions occurred, meanwhile communication team asked the projects to verify. After this phase, the communication team consulted the projects after which the case studies were published.

Publish on the website, CONNECT magazine and social media

As a result of the effort gathering the case studies they were published on several platforms:

- The primary place of publication is the NGI_Trust wiki. The case studies have been placed on the wiki to have all information regarding NGI_Trust in one central location:
  - *https://wiki.GÉANT.org/display/NGITrust/Case+Studies*
- GÉANT's magazine CONNECT 36 pays attention to the first three case studies;
  - *https://connect.GÉANT.org/wp-content/uploads/2021/03/GÉANT_CONNECT_36_single_page.pdf.*
- The publication in the CONNECT 36 magazine received attention in communications on Twitter.
- The case studies were also promoted on the NGI_Trust Twitter page and distributed to the project partners.

Furthermore, a blog post was written about the case studies or the GÉANT connect page and the NGI_Trust wiki:

- GÉANT connect magazine:
  - *https://connect.GÉANT.org/2021/08/18/a-look-at-new-advancements-in-privacy-and-trust-in-six-new-case-studies-by-ngi_trust*
- *NGI_trust wiki blog:*

- *https://wiki.GÉANT.org/pages/viewrecentblogposts.action?key=NGITrust*

Subsequently, we also communicated to the projects that the case studies had been published (Annex 2, Email 3).

3.2 Results and discussion / Perspectives

The main outcome of this activity was to have published the case studies, which has been successful. In total nine different case studies for 11 different projects have been published. The reason for having nine case studies from 11 project is that two project teams applied for funding in different open calls.

https://wiki.GÉANT.org/display/NGITrust/Case+Studies

Moreover, the following tweets have been created about the case studies:

Figure 1: Tweet CONNECT magazine

https://twitter.com/NgiTrust/status/1376825199350456324

Figure 2: Tweet new case studies

https://twitter.com/NgiTrust/status/1428003385551335426

Name	Lead (Task Leader)	% complete	Delivery project month	Comments
Create template	GÉANT	100%	M22	Done
Selecting case studies	GÉANT	100%	M23, M25, M27	Done
Approaching projects	GÉANT	100%	M25, M27, M29	Done
Cleaning up case studies	GÉANT	100%	M27, M29, M31	Done
Publishing case studies	GÉANT	100%	M29, M31, M33	Done

3.3 Maintenance and/or next steps / roadmap

In addition to the publication, the NGI_Trust communication team has communicated the results back to the project teams to use the case studies as well in their communication.

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

4 Conclusions

To conclude, the case studies has been published successfully. In addition, the results are communicated to the project teams with positive reactions and feedback on the guidance of creating the case studies with a pre-created case study template.

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

Annex 1: Case study templates

NGI_Trust case study template

NGI_Trust Case study

Introduction

The **Next Generation Internet (NGI)** is a European Commission initiative that aims to shape the development and evolution of the Internet into an Internet of Humans. An Internet that responds to people's fundamental needs, including trust, security, and inclusion, while reflecting the values and the norms all citizens enjoy in Europe. NGI Trust is part of the NGI family; also have a look at all the other initiatives taking place at https://www.ngi.eu

As part of NGI trust, we would like to congratulate you on being selected to participate in the NGI_Trust case study. It is extremely appreciated that you are willing to participate. We would like to invite you to write a case study using the following template. The purpose of this is to showcase the wonderful work you have done and will be doing as part of the NGI_trust project. The case study will be shared with the partners in the NGI_Trust network and beyond the NGI network, through websites and social media communication channels.

Guidelines:

By creating this template, we hope to assist you in writing the case study, we created guidelines and a case study format to have all the case studies consistent.

Requirements:

- 800-1500 words
- Optional questions to answer are marked with: **[Optional]**
- Questions may be merged or can be answered simultaneously
- Try to create a nice story instead of answering questions separately
- Please sent along multiple pictures that could be used in communications (e.g., Twitter/blog and wider spread):
    - Pictures or graphical material or prototype screenshots.
- Please submit before **<DATE>**

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

Case study template

Title

<title>

Summary

<abstract with highlights of the project>

Keywords

<provide a few keywords>

Actors involved in the project

<*Who are the partners and persons involved in the project>*

Case study questions:

<Please use the following questions and create a story that is nice to read>

The business

- Tell me about your project – what industry/area you are in and what does your business/project do?
- What can you tell me about the actors involved in the project?
- Can you provide some figures about your organization, such as size, (*turnover - optional*), number of staff, office locations?

The problem

- What was the problem (technological/business/privacy-related) you were trying to solve?
- Was there a particular trigger that made you decide it was time to act?
- What were the key challenges you needed to address?

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

The solution

- When did the project begin and end?
- What were your project objectives?
- What technologies were used?
- What is the business model?
- What was the process of developing the solution?
    - Please also provide the technical details **[Optional]**

- In what way does your project contribute to a human-centric internet?
- What does privacy mean to you? **[Optional]**
- Explain why your project is competitive in related to other alternatives

Results

- How is the solution now being used?
- Has it achieved the project objectives?
    - And how do you measure, what are your KPI's? How do you evaluate?
- What quantifiable benefits can you attribute to the solution (e.g., return on investment)
    - What kind of success did you achieve in your project?

- What other business benefits have you experienced as a result of this project?
- How does this compare to how you were doing things previously? **[Optional]**
- What does your project contribute to the European ecosystem of researchers, innovators and technology developers in the field of privacy?
- How have users reacted? **[Optional]**
- What roadblocks for implementation did you overcome?

Testimonial

- How has the NGI_trust project helped since implementation?
- What did you learn from the NGI_trust project? **[Optional]**
- Why did you apply to the NGI_Trust project? **[Optional]**
- How did the coaching sessions influence the work?
- How would you describe your relationship with the coaches?

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

- If you were to recommend the NGI_trust project and possible other NGI initiatives, why would you do this?

Future plans

- Do you have plans for future development?
- Off the back of this project, are there any other projects either underway or in the pipeline?

If you have questions about the template don't hesitate to contact us on auke.pals@GÉANT.org

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

Annex 2: Email templates

Email 1

Dear **<name>,**

Hope you're doing well; we selected your project **<project>** for our NGI_Trust communication campaign, congratulations!

We would like to give you more exposure by creating a case study from your project. My question to you is if you're open for that, writing a 1-page case study? After confirmation I will send you a template which could help creating this case study.

If any questions, please reach out,

Best,

<name>

Email 2

Dear **<name>,**

Hope you are doing great, I'm happy hearing from you and also your interest to participate in the case study. All the information about how to write the case study and in which format can be found in the attached template. Concerning the deadline, our communication department requested to have the case study ready by the **<date>,** hope you can make it by then!

Attached you can find the template. If having any questions please let me know, if needed we can setup a call.

<attachment>

Best,

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

<name>

Email 3

Dear all,

Herewith you can find the full case studies published,

https://wiki.GÉANT.org/display/NGITrust/Case+Studies

our partners will distribute them further, they're also included in the CONNECT magazine: https://connect.GÉANT.org/wp-content/uploads/2021/03/GÉANT_CONNECT_36_single_page.pdf

Interactive version:

https://indd.adobe.com/view/16e0c72b-66d6-4e67-b0a9-76fee4916ef2

Kind regards,

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

Annex 3: Case Studies

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

Better Internet Search - The ISIBUD Project

Summary

Better Internet Search project ISIBUD was supported by the Next Generation Internet - NGI Trust project. The project was run in collaboration with Edinburgh Napier University and was completed in July 2020. This resulted in a demonstrator for a unique ad-free privacy-preserving search engine being tested with 100+ live users.

The success of this project has led to the search engine being publicly released as an MVP and it continues to be developed by the company partly supported by a second grant from the NGI Trust. A future release with blockchain used to secure the token-based economy is planned for summer 2021.

Keywords

Search Engine, Privacy-preserving, Google, user focussed

Actors involved in the project

Better Internet Search Ltd collaborated with Edinburgh Napier University to deliver this project and is working with Danish company Partisia Blockchain to deliver the second ongoing project.

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

The project

Figure 1. Dr Gordon Povey

Better Internet Search Ltd (BIS) was founded in 2019 by serial technology entrepreneur Dr Gordon Povey with the aim of developing a more user-focussed search engine, where personal data does not need to be gathered centrally and the user has inherent privacy and control of their data. The foundation of the business was laid after receiving funding from the NGI Trust in late 2019. A small development team was formed which included technical support from Edinburgh Napier University (ENU).

With two part-time staff from ENU and two full-time, plus two part-time staff from BIS the platform was created and by the end of the project in July 2020, it was demonstrated using live users. The development continued beyond the end of the project and BIS launched an MVP version of the alternative ad-free search engine to paying customers on 22nd December 2020.

The business has now received additional funding allowing the development of its alternative revenue model which will deliver a privacy-preserving, ad-free search engine requiring no paid subscriptions. There are only a couple of hundred live users on the current platform, but this will be ramped-up significantly once the revenue model has been suitably refined for profitability.

The project aim was to build a demonstrator for the proposed alternative search engine. In collaboration with ENU, a platform which delivers Web searches as well as Image and Video searches was developed. The follow-on project's aim is to deliver the ad-free monetisation model and to secure the token economy system via blockchain.

The problem

The problem with current search engines is that you have become the product that they sell to advertisers, the ads are becoming increasingly unsafe with clickbait, fake news, phishing scams and the danger of filter bubbles. Privacy-preserving search engines such as Duck Duck Go and Ecosia do not harvest your personal data, but you are still exposed to the same unsafe advertising content. The results and general user experience are not well differentiated from the incumbent search engines like Google and Bing.

To achieve proper differentiation (and potential market disruption) we needed a search engine that is not only privacy-preserving, but that makes searching safe again. We need a user-focussed search engine where the user is the only customer to be served. We decided to build our alternative search engine based on a belief that an alternative revenue model exists that does not include advertising.

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

Our initial key challenge was to build a platform on which we could develop our new revenue model, and this required building an alternative search engine that our target customers would consider to be better than the incumbents' products. The second challenge was developing a working prototype of the alternative revenue model on this platform.

The solution

We began the project in August 2019 with the objective of delivering a demonstrator for our alternative search engine by July 2020. This would include demonstration of the alternative revenue model.

The project was built on the Azure cloud platform and utilised API access to Microsoft's comprehensive database of indexed URLs, which is essentially the same database used by the Bing search engine. We developed our own methods to process and present the data, allowing for future machine-learning work which can further improve the ranking of results.

The business model is unique and instead of advertising, where attracting user clicks is the primary metric, we developed an alternative brokerage model where delivering the requested results becomes the key metric. When there is a cost to delivering results we charge a fee (in the form of tokens), whereas, in the case where a search results in online sales, we can generate a revenue and credit multiple tokens back to the user. With worldwide online sales growing rapidly but on-line advertising revenues slowing, we believed our alternative ad-free model could now be viable. Thus, it was built into the demonstration system to prove its technical viability and to enable it to be further developed and refined.

Results

The final demonstrator was delivered at the end of the ISIBUD project in July 2020. It had been alpha tested with over 100 live users – mainly in the UK but including English speaking users in a number of different countries. The final version included general web search, image and video searches and the prototype of map and product searches. The token-based economy was also implemented enabling users to gain tokens via product searches as well as spend them through organic search.

Figure 2. Better Internet Search interface and search results

The project enabled us to demonstrate a unique user-focussed search engine that is both privacy-preserving and completely ad-free, and which aligns well with the values of the

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 project. Following completion of the project it was developed into a beta version and a minimum viable product (MVP) version was released publicly on 22nd December 2020. As the product search monetization model was in early prototype form this was removed from the MVP and instead early users purchased tokens.

The development of the monetization has continued towards a commercial build phase supported through additional grant funding from NGI Trust, and in collaboration with a new European partner, Partisia. This project will enable the search engine to be released commercially with the new monetization model fully operational via a cooperation with the company Kelkoo (beta release due in May 2021) and secured via blockchain technology (final release due in July 2021).

Testimonial

Developing a new user-focussed search engine is considered bold and risky, but NGI Trust were willing to support this, and the end result has clearly been very positive. The coaching and support for IP and networking has been excellent and resulted in the plans evolving into a commercially viable roadmap.

Computing magazine recently tested the search engine and noted “Computing tried the Beta, and it is certainly very quick and accurate, although of course this was not the production version.”

The follow-on support funding from the NGI Trust has enabled the original demonstrator platform to be turned into a commercially viable product that will be released in 2021.

Future plans

On the conclusion of the current commercial project supported by NGI Trust, the company will release a new version with the full product search supported business model and with the token system secured on blockchain technology. The search engine is potentially disruptive because it is the first such product to have a working monetisation model that is both ad-free and subscription free. Further developments will focus on localising searches, especially product searches, enabling users to easily find sustainable and more locally sourced products, and to rank results by a number of ethical metrics.

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

CAP-A: A Community-driven Approach to Privacy Awareness

Summary

Solid legal regulations and technical countermeasures are not always sufficient to achieve society-wide impact on privacy protection; data protection can also be powered by the society itself.

The CAP-A project is offering socio-technical tools to promote collective awareness and informed consent, whereby data collection and use by digital products are driven by the expectations and needs of the consumers. Theme-driven events aimed at rating the privacy friendliness of apps of specific categories and at annotating their Privacy Policy documents have helped us generate informative statistics about the behaviour and mindset of citizens and the privacy-consciousness of mobile apps.

Keywords

Collective Awareness, Mobile Apps, Privacy Expectations, Privacy Norms, Privacy Policy Annotations.

Actors involved in the project

CAP-A is run by two partners (see https://cap-a.eu/), namely the Foundation for Research and Technology – Hellas (FORTH) and IN2.

FORTH coordinates the project and participates with the Institute of Computer Science (ICS) and the PRAXI Network. IN2 Digital Innovations, is a software development company offering web-based solutions.

Contact Persons

Theodore Patkos – patkos@ics.forth.gr
Giorgos Flouris – fgeo@ics.forth.gr
Ioannis Chrysakis - hrysakis@ics.forth.gr
Alexandru Stan - as@in-two.com

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

The business

Privacy and anonymity in the digital world are becoming increasingly difficult to achieve. While we recognise the dramatic progress brought about by Information and Communication Technology (ICT) in almost every aspect of our everyday life, we realise that, in the process, we handed over privacy management to businesses and corporations that are primarily driven by a profit motive, making our personal data vulnerable to exploitation in ways that are harmful to us. As ICT scientists and as citizens of the digital world, this situation has been causing us a growing feeling of discomfort.

Four years ago, we decided to take some action. Driven by FORTH-ICS and supported by IN2 and a number of other academic and industrial entities, as well as individuals, we launched the CAPrice initiative, a grassroots community with the goal of applying crowdsourcing solutions to raise awareness and provide solutions to privacy-related matters. The CAP-A project is part of this initiative.

FORTH (Greece) is the largest research centre of Greece. FORTH-ICS has a long track record in conducting basic and applied research, occupying a full-time staff of over 350 people. FORTH also involved the PRAXI Network in the CAP-A project, a distinct administrative unit operating within FORTH, and an established technology transfer organization.

IN2 (Germany) provides extensive experience in applied research and innovation, building cutting-edge webware and scalable solutions for the Web.

The problem

Society in general acknowledges that privacy preservation is essential in human relations, democracy, independence, and reputation. Yet, for various reasons, the more pronounced being limited awareness of the involved risks, we tolerate untrustworthy software to collect, store and process our data, having limited or no evidence as to how this sensitive information will be protected, who has access to it, or even what the intended purpose is.

The need to forge sound laws to regulate business policies for data protection is judged necessary; but, unfortunately, solid legal regulations are not always fully capable of accomplishing a paradigm shift. The ease with which we give our consent to the processing of our data not only hinders the efficacy of legal regulations, but also makes it difficult for technical countermeasures to achieve a broad impact on privacy protection.

We therefore proposed to NGI_Trust the CAP-A project, at the heart of which is the hypothesis that data protection can also be powered by the society itself. By mobilising consumers to become active players in digital marketplaces and by developing tools to harness our collective power, the adoption of the technical and regulatory frameworks can become more effective and ubiquitous, and the market will act with responsiveness, mostly because it is profit-maximizing.

CAP-A is offering socio-technical tools to promote collective awareness and informed consent, whereby data collection and use by digital products are driven by the expectations and needs of the consumers themselves. Apparently, the biggest challenge faced when putting community-driven efforts to action is to engage a wide and diverse audience, and at the same time to stimulate the participation of various stakeholders in

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

the process. As a result, our team devoted equal effort both to the technical and to the societal aspect of developing the CAP-A solution.

The solution

CAP-A began in August 2019 and was planned to run for one year; however, due to the COVID-19 pandemic, an extension until the end of 2020 was granted. The goal of the project was from the beginning threefold.

First, we developed a **suite of ICT tools** to facilitate the participation of users in accomplishing tasks related to privacy aspects of mobile apps. The CAP-A portal and the CAP-A mobile app encapsulate, among others, services for app search and rating, Privacy Policy annotation, community analytics and a news corner. The portal provides the means to generate useful privacy-related content for all members of the community. The CAP-A tools were implemented using open-source technologies, such as Virtuoso for the global repository, JAVA and REST for the web services and Swagger for testing and documentation.

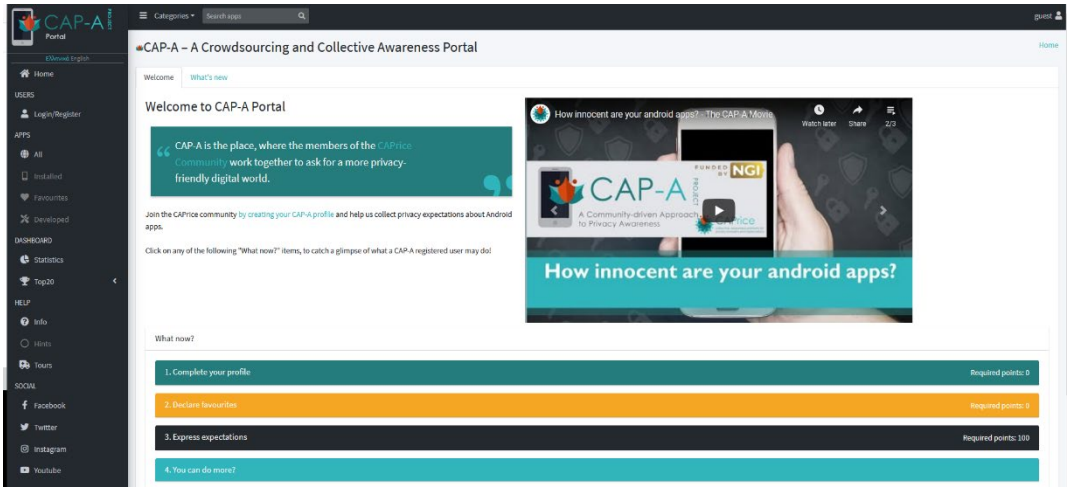


Figure 1. The CAP-A Portal

Second, we designed and implemented a **gamification/rewarding strategy** to increase user engagement and to motivate participation and contribution. Building and sustaining a community is a key success factor of any crowdsourcing solution. We therefore enacted a strategy that rewards the time and effort contributed, which is tailored to the ICT tools developed and fun to experience.

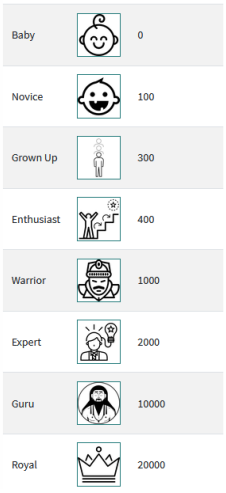


Figure 2. CAP-A Tiers

Finally, we organized **pilots** in the form of **thematic events**. In collaboration with external collaborators, we launched 6 events, where users could express their opinion about apps of specific categories, such as game apps, social media apps, conferencing apps etc. The focus of our campaign targeted primarily simple users, but we also ran pilots for legal experts, as well as with app developers, in order to attract the participation of various stakeholders. Among similar projects, CAP-A is probably the first effort to truly mobilise community action on such a scale, by applying both aggregation and co-creation actions.

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

Throughout the project, the CAP-A team considered various potential business models. We concluded that the establishment of a separate legal entity (NGO) with a dedicated social profile can incorporate several possibilities for revenue generation (licensing and cooperation agreements, advertising, consultancy and training, data analytics provisions, public grants and private donations). It will also better serve the principles and concepts of the CAPrice initiative.

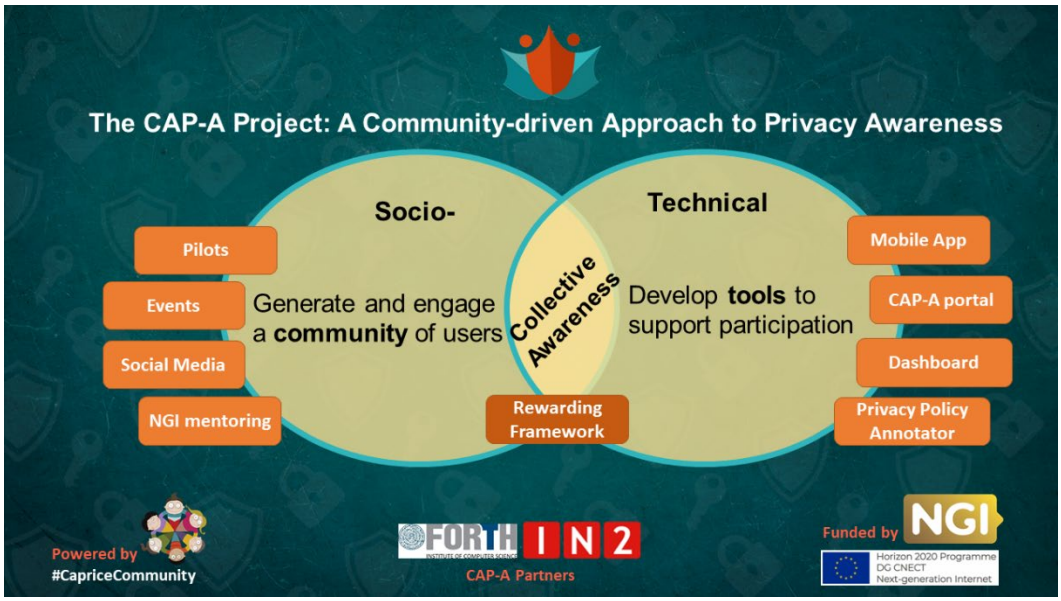


Figure 3. The CAP-A Solution

Results

The CAP-A portal digested privacy-related information about more than 19K Android apps, which is available for users to explore. During the project, 164 users registered and used the CAP-A portal, whereas 51 users installed the mobile app. Their contributions resulted in the expression of personal expectations for about 567 apps and in 1181 annotations on different Privacy Policy documents.

Beyond the portal and the project website, our communication and dissemination activity reached 253516 Facebook users and 34468 Instagram users, while our official twitter account made 104.3K impressions. It also helped grow the CAPrice Community, namely the mailing list by 240% (currently 455 users) and the total community size, including social media followers, by 142% (currently 1555 users/followers/subscribers). Moreover, we presented the CAP-A project in 7 scientific venues and 12 wide public events.

Considering the above, one of the main objectives set in the beginning of the project, i.e., to attract the interest of a considerable number of users to start generating informative privacy norms, has been achieved. The CAP-A dashboard provides a wealth of statistics, as for example the percentage of citizens who found reasonable to give access to a certain type of data, such as camera or contacts, for a given app category. This information can be used by different stakeholders (developers, social scientists, policy makers) to conduct analyses and interpret the behaviour and mindset of various user groups, according to age or other demographic characteristics.

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

The CAPrice community is not a sizable virtual community yet; the biggest challenge is to achieve the critical mass needed to make the community self-sustainable. Already the experience gained during the course of the CAP-A project led us to improve and adapt our user enactment strategy at various levels.

Testimonial

The idea behind CAP-A existed long before we became aware of the funding opportunities offered by the NGI_Trust project. As the expected impact and objectives of the call matched perfectly with our objectives, we decided to apply.

This turned out to be a very good decision, as our overall experience from the cascade funding mechanism and collaboration with the NGI_Trust project is judged very satisfactory. The short period between proposal submission and beginning the actual work, the clear requirements, and the swift management of the administrative procedures helped us focus on the important aspects. In addition, the frequent -yet not overwhelming- communication with the NGI_Trust coordinators and our mentors (coaches) created a feeling of teamwork.

During the course of the project, we participated in the "NGI_Trust business mentoring and IPR support" webinar, followed by a series of one-to-one sessions with the organizer, Unai Calvar Aranburu. The outcome of these communications was helpful and positive. We also valued as really important the networking sessions that NGI is constantly organising. It enables us to meet the people behind the NGI Initiative, as well as members of other third-party projects, people with whom we share common ideas regarding privacy and trust in the Internet.

Mentoring was provided by two coaches, namely Colin Wallis and Alejandra Ruiz, the collaboration with whom was seamless and warm, and was based on mutual respect. In all 3 virtual meetings that we had, the coaches confirmed the good state of the project and gave us useful feedback and comments for further improving our work. Moreover, we engaged the coaches in several important decisions and looked for their advice and feedback in critical deliverables. Mentoring was initially perceived by the project members as a way to ensure the good state of CAP-A and its smooth running at specific checkpoints (similar to project reviews in EU projects). However, mentoring turned out to be much more than that, as the coaches' feedback helped steer the project towards its successful completion and was valuable in more ways than just as a reviewing mechanism.

Future plans

The CAP-A project is part of/and predated by the CAPrice initiative. Through CAPrice, the outcomes of the project will be maintained in the future. However, to fund additional development and feature improvements, other sources of income should be considered. Towards this aim, we will employ in parallel two complementary approaches.

The first is to pursue the chosen exploitation path for the CAP-A project, which consists in the establishment of a Non-Profit Organisation (NPO), acting as an umbrella that will

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

incorporate additional identified possibilities for revenue generation. The generated income will be leveraged for further investments that will enlarge the scope of the CAP-A tools and CAPrice initiative and will support future development. A further exploitation opportunity (that could be served through the NPO as well) is the idea of selling licenses to specific stakeholders, in order to use certain parts of the database or to open up part of the data through an API for providing added-value services over CAP-A.

The second approach consists in seeking additional funding for some follow-up project. Towards this, we are considering various calls, both national and European, including other cascading funding opportunities within NGI.

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

CASPER-2.0: An AI-based ghost protecting children from online threats

Summary

The main aim of the CASPER-2 project is to develop an artificial intelligence-based application-agnostic agent operating on user-interface human-computer interaction level to detect & prevent inappropriate content for children.

Keywords

Application-agnostic solution, artificial intelligence, children protection, human-computer interaction, software, online child protection.

Actors involved in the project

- Serbia (School of electrical engineering): Aleksandar Jevremovic, Milan Cabarkapa, Marko Krstic, Mladen Veinovic, and Milos Stojmenovic

  The School of Electrical Engineering in Belgrade has over a century-long history of education and research in the fields of electrical engineering, telecommunications, and (later) computer science. Over 1.000 students enrol every year.

- North Macedonia (Faculty of Computer Science & Engineering): Ivan Chorbev, Ivica Dimitrovski, Petre Lameski, Eftim Zdravevski

  The Faculty of Computer Science and Engineering (FCSE) at UKIM is among the largest and most prestigious faculties in the field of computer science and technologies in North Macedonia. It started to work in 1985 under the name "Institute of informatics".

- Portugal (O Mundo da Carolina): Nuno Garcia, Nuno Pombo

  O Mundo da Carolina is a non-profit association that aims to support children with chronic diseases and who are in an unfavourable socioeconomic condition.

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

The project

Our project started in a less developed area, with the main objective of protecting children and young people using the Internet.

At first, we just discussed the possibilities of using AI on the human-computer interaction (HCI) level to create an application-agnostic solution for filtering inappropriate content. Our team members - scholars from Serbia, North Macedonia, and Portugal - already had a great experience in domains like cybersecurity, human-computer interaction, and artificial intelligence. Then, we found a NGI Trust call and we decided to apply, sending our proposed solution. As the proposal was accepted, we obtained funding and we also got the chance to work with great people and field experts like Mr. Alasdair Reid, Sigita Jurkynaitė, Javier Nesofsky, Raffaele Buompane, Christian Schunck, and Casper Dreef.

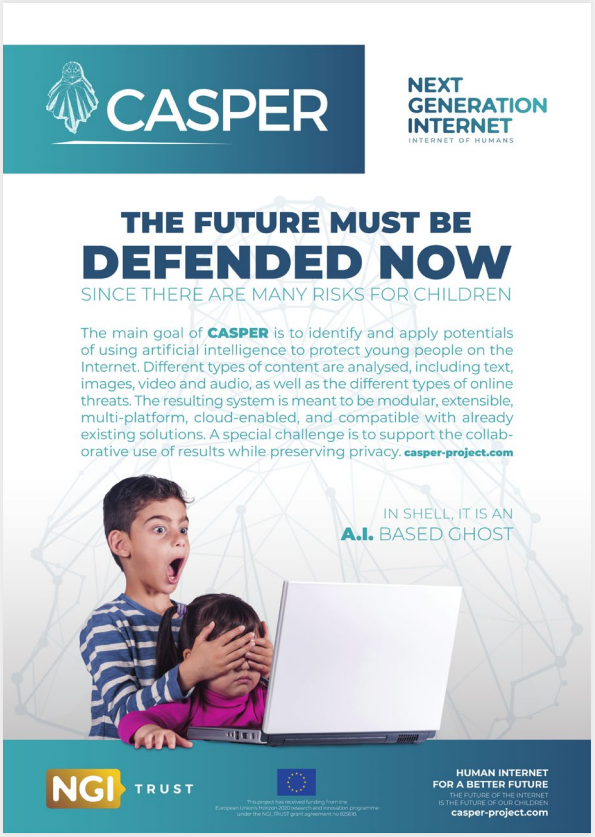


Figure 1. CASPER poster

The problem

Our project aims to provide an application-agnostic solution for filtering inappropriate content from online communications. This means to detect the inappropriate content and, where applicable, to prevent exposure of this content to end-users.

Figure 2. CASPER project members at the kick-off meeting in Belgrade, Sept. 2019

At the very beginning, since most of our researchers are parents of young children and adolescents, they tried to apply existing solutions to protect them when using the Internet. It was surprising to discover that there was no effective solution available to cover different applications and different threat types. So, our original idea and our research started somehow to scratch this personal itch. Later, the COVID-19 pandemic showed us how necessary and critical this project was, since people - including the most vulnerable groups - were spending even more time online.

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

Originally, within the **Casper 1.0** project, we mostly focused on protecting young children from being exposed to nudity, pornography, and online cyberbullying. In other words, we developed and tested algorithms to be integrated into a compact product.

After this step, we received a grant for **CASPER 2.0** in order to implement the results from CASPER 1.0 viability study. The main focus of the second project was to achieve real-time performance and complete a Minimum Viable Product.

During the project we faced many challenges, including selecting effective and efficient algorithms, optimizing to achieve real-time performance, protecting users' privacy in distributed classification scenarios, getting relevant training datasets, etc. The bright side is that overcoming some specific problem usually gave us additional ideas on how to expand or improve the project.

In fact, after testing different algorithms and developing prototypes, we understood that the potential of our original approach was much bigger. As such, within the Casper 2.0 project we expanded the scope to support other languages other than English, and to protect another vulnerable user profile: elderly people. Of course, from completely different types of threats - fake news and online frauds.

The solution

The Casper 1.0 project started in August 2019 and ended in July 2020. Casper 2.0 started in August 2020 and ended at the end of April 2021. Our main objective was to develop an application agnostic AI-based solution on HCI/UI level to detect/prevent inappropriate content for children.

During the Casper 1.0 project, we made the first steps in recording HCI and then post-processing it to select optimal algorithms. Within the Casper 2.0 project instead, we focused on achieving real-time performance, by optimizing architecture, using dedicated hardware, or using edge-computing architecture.

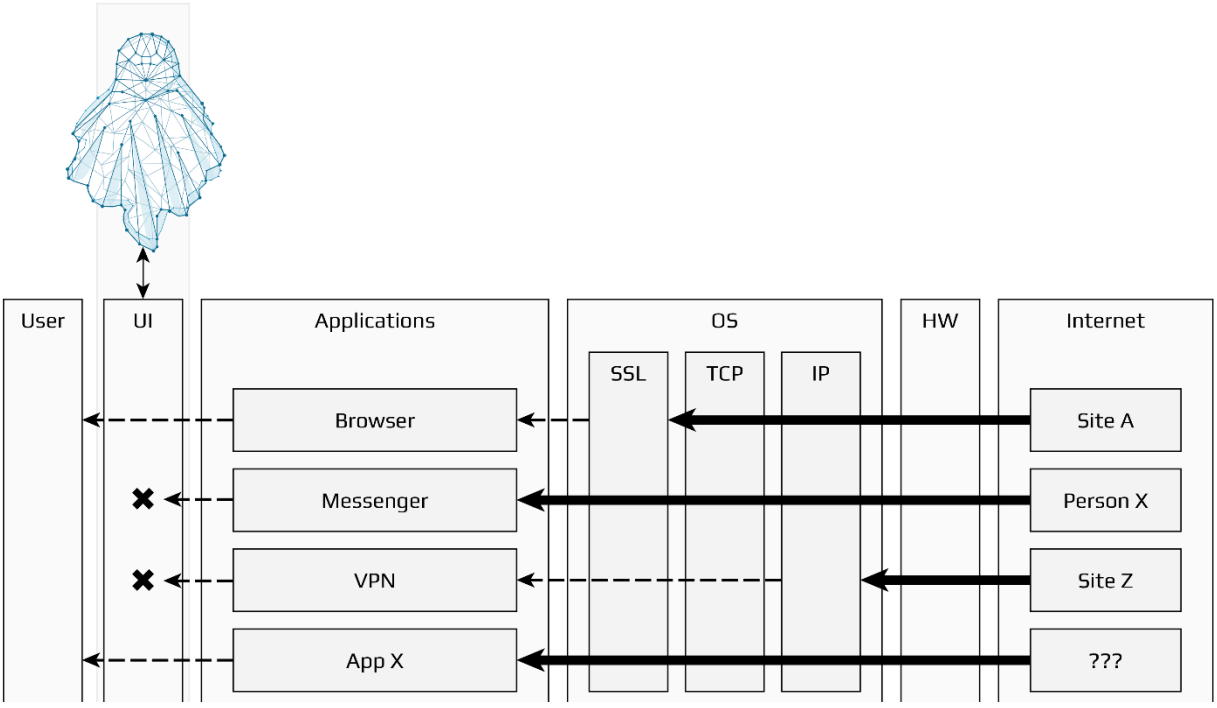


Figure 3. Example of content filtering via CASPER

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

While working on our solution, we used different programming languages (Python mostly) to develop new algorithms and the platform, and different existing algorithms for OCR, text/image classification, etc. We also used WireGuard as a VPN solution for edge-computing scenarios. The MVP product is developed for Windows OS. Some features (for instance screenshot capturing and UI reaction) need to be adapted for different desktop and mobile platforms. We plan to support Android and Linux in the future.

One of the main CASPER use-cases is related to the use of messaging apps. Although many social network platforms implement mechanisms for protection from inappropriate content, their messaging part is still vulnerable. One of the reasons for that is that the same mechanisms cannot be applied without endangering users' privacy and bypassing end-to-end encryption used in messaging apps. However, CASPER agents could provide children protection even for these applications by analysing content completely locally on end devices. This way both privacy and encryption issues can be overridden, providing application-agnostic protection to our children.

Our idea is to make this software available to anyone who needs this kind of protection, regardless of their economic situation. On the other side, it is critical to prevent this software from becoming mass surveillance software. So, going open source turned out to be the only possible choice. Thanks to NGI we were able to develop a functional prototype. When the funding from NGI stops, we plan to continue our work as a foundation, and we expect our primary source of income to be donations.

Our project is competitive in relation to other alternatives mostly because of its holistic and application-agnostic approach. Practically, it means that even if someone manages to overcome the DNS protection or to inject malware to the victim's computer, our software will still manage to protect them from revealing personal data or being exposed to inappropriate content.

We strongly believe that protecting children and other vulnerable categories when using the Internet is one of the critical tasks for creating a better society and better Internet. Going open source is also a critical aspect of that belief.

Privacy means protection from threats that we are (still) unable to fight effectively. That's why vulnerable groups of Internet users, including children and elderly people, need their privacy to be respected. In some cases, it even means preventing them to perform some actions - actions that could be harmful to them, but that they are not in a position to recognise.

Figure 4. Aleksandar Jevremovic, Professor at Singidunum University in Serbia, researcher at the School of Electrical Engineering in Belgrade.

Results

Since it is a "mission-critical" software, we are very cautious about releasing it in public. At this moment, we have the software running on some personal computers that our researchers can control. However, we have to do some additional optimisations, in terms

of efficacy and efficiency, before we are sure that it can provide the required level of protection to end-users.

Our current metrics mostly depend on the quality of datasets we use for training the algorithms. Because this is a very sensitive topic, we can't do testing with real users. When we release the software in public, we'll also use false positives/negatives as relevant metrics.

We presented our project at different conferences, and the reactions were mostly very positive. Especially in cases where young parents were eager to download and test the solution. We consider this to be a success we were striving for since the beginning of the project. On the other side, since our goal is to make this software freely available, if we manage to continue our work based on donations, we'll consider that to be another big win.

Considering its open-source nature, our project can also be seen as a research framework in this field. This means that other researchers can use the project as a base for their research. Preserving privacy is one of the critical goals of this project, and the open-source license is a way to insist on that.

Testimonial

Projects like ours, that are oriented towards the common good but are not profitable, are not usually very interesting for investors. Regardless of that, the NGI Initiative decided to support our work on the project, not only by funding researchers but also by providing mentors, coaches, consulting, access to relevant events, training, webinars, connections, and much more.

We received great help from our coaches and mentors. Since our team is mostly made of researchers and scientists that lack relevant business experience, they helped us to find business models that would fit our needs. Also, they helped us to consider other aspects, especially those relevant for providing project funding in the future.

We had some very basic questions in some domains, but the coaches were more than patient to guide us and give us advice on how to overcome some difficulties we faced during the project.

Future plans

We will try to continue our work as a foundation, and we already had some interesting talks with UNICEF, the WeProtect Global Alliance, and others. As soon as we have a functional prototype, it will be much easier to attract funding.

Additionally, we already have some ideas to apply a future CASPER foundation in other domains, but we are currently too busy working on this project. Even if we had more developers and researchers, we would use them on this project. There is a lot of work to be done in the next 5-10 years.

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

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*

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

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.

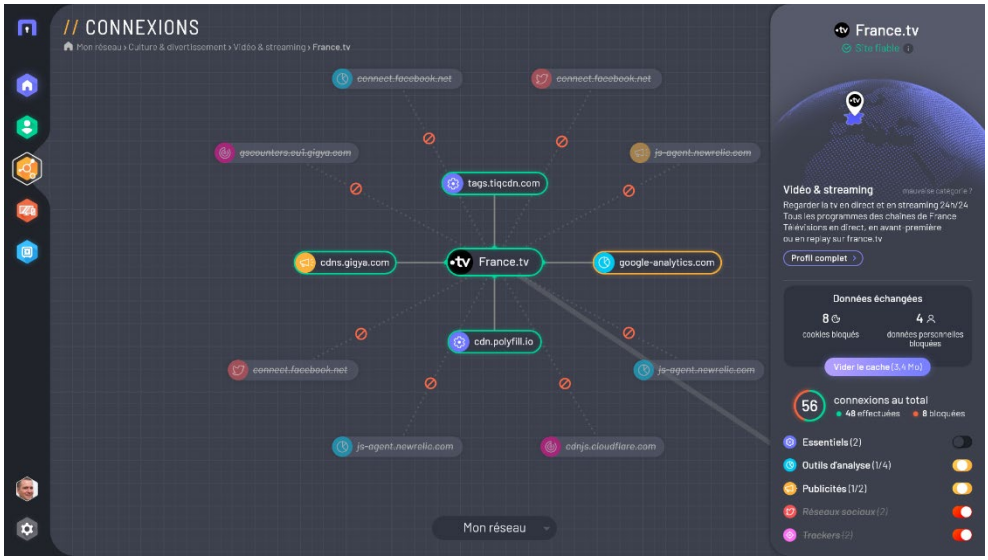


Figure 1. PyGuard Interface showing overview of all network activities.

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.

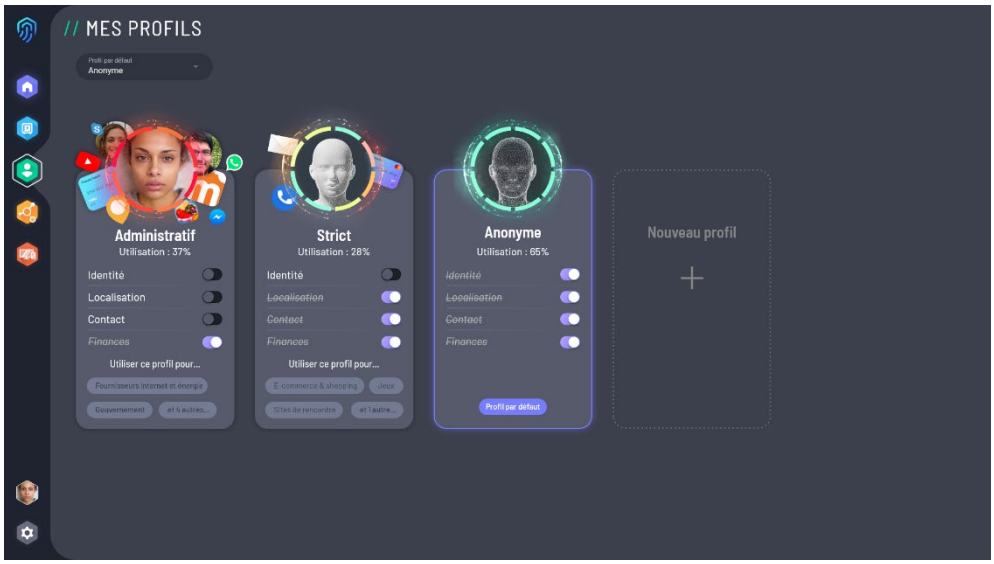


Figure 2. Digital Personal Avatars

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

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.

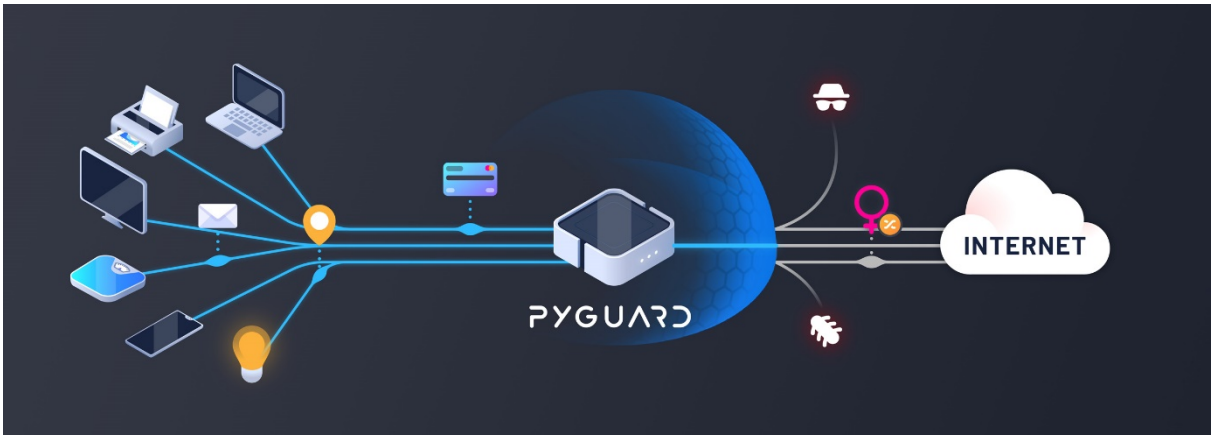


Figure 3. The PyGuard Solution

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

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

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

SensifAI: Smart-enhancing videos and images on-device while fully preserving privacy

Summary

There are many different image enhancement apps (e.g., Letsenhance.io and Google DeepAngel) that improve the quality of images or edit them automatically through advanced artificial intelligence. These apps require users to send their images to their cloud to process them. This increases the risk of getting hacked, exposed, or abused and potentially violates the privacy of millions of users. This is all because these apps work based on deep-learning that is computationally heavy and requires strong GPU servers.

SensifAI offers a game-changing technology that solves this problem. We have developed specific deep learning architectures for the new NPU chipsets of most major smartphone manufacturers. With this technology, we can enhance users' images and videos locally on their mobile phone without any connection to the internet.

In this project, SensifAI delivered an on-device, smart-enhance app that can help millions of people enhance their video/image archives while guaranteeing control over their personal data. We will also add automatic and real-time face and vehicle license plate detection/blurring systems in future versions of the app such that users can avoid unwanted violation of other people's privacy in public areas while live broadcasting or sharing images/videos on the internet.

Currently, SensifAI forged a partnership with worlds top semiconductor companies (Intel, NVIDIA and Huawei) that supply processors and AI chipsets to smartphone manufacturers and seized the opportunity of deploying deep-learning algorithms on NPUs for the first time in the world and publicly launched the world's first all on-device, deep neural and real-time video recognition application.

Keywords

Video Enhancement, Deep Learning, Edge Computing, Embedded Deep-Learning

Actors involved in the project

Mohamad Hasan Bahari, Ali Diba, Luc Van Gool

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

The business

SensifAI develops cutting-edge deep learning technologies to recognize video and images automatically. SensifAI has launched the world's first embedded video recognition App for NPUs publicly and was a launch partner of Amazon Sagemaker platform and released the world's first customizable video recognition platform.

SensifAI has gigantic customers such as Huawei, and Artus and world leading technology partners such as Amazon, NVIDIA, and Intel. The company has won several awards including EU top 50 company award, MIT technology review top 10 innovators in Belgium and IUIA innovation award. The company was founded by three alumni and scientists from MIT, ETHZ and KU Leuven, who previously co-founded over 10 successful start-ups. Having worked in the same research lab before SensifAI has helped the leadership team to develop a strong bond.

The problem

There are many images in our albums which are far from ideal due to bad lighting conditions, low resolutions of old cameras, or incorrect automatic setting of the camera. At the same time, there are different image enhancement apps (Letsenhance.io and Google DeepAngel) that improve the quality of images or edit them automatically through advanced artificial intelligence. These apps require users to send their images to their cloud to process them. This increases the risk of getting hacked, exposed, or abused and potentially violates the privacy of millions of users. This is all because these apps work based on deep learning that is computationally heavy and requires strong GPU servers.

The SensifAI solution and its results

SensifAI Image and Video Enhancement App automatically improves your low-quality images using an advanced artificial intelligence (AI) method based on deep neural networks. This app offers a fast and end2end approach to increase the lighting in dark pictures, improve contrast and brightness, shoot up the resolution, and adjust tones.

The software which is publicly available as an SDK as well as an Android App works in three modes: **automatic enhancement**, **superresolution**, and **manual improvement**. One can use one of these modes to enhance a specific picture according to a required correction and modification.

In **automatic enhancement** mode, the software applies a deep-learning model to automatically improve your image quality. For example, it increases the lighting of the images and improves the brightness without any effort from the users. Then it shows both images before and after the enhancement and lets the user compare them and save the enhanced image or remove it.

In **superresolution** mode, the program helps to increase the resolution of the images automatically using a deep-neural network system.

In **manual improvement** mode, the software provides a set of tools such that the users apply different filters manually to re-color or adjust the brightness of the picture. This mode is also accessible after an image was treated in superresolution or automatic enhancement modes.

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

SensifAI offers a game-changing technology that solves this problem. We have developed specific deep learning architectures for the smartphone chipsets of most major smartphone manufacturers. With this technology, we can enhance users' images and videos locally on their smartphones without any connection to the internet. This is an on-device, smart-enhance App that can help millions of people enhance their video/image archives while guaranteeing control over their personal data.

The main advantages of SensifAI enhancement app are:

Guaranteeing User Privacy	Since SensifAI runs on the device, no personal data will be exposed to the cybersecurity risks of cloud-based platforms and users will have full control over their data.
Cutting the Costs of Cloud-Processing and High-Speed Internet Connection	Our app processes all the data locally on the user's smartphone and thus cuts the (in)direct costs of cloud computing on expensive GPU-servers. This is because central computation over GPU-servers is very expensive and our app cuts the users' costs for cloud computation.
No Need for High-Speed Internet Connection	Since the data is processed locally in the device, there is no need for an internet connection. While competitor apps require users to use the Internet to upload large video/image files to their cloud. This also reduces the costs for users.
Enhancing Videos as well as Images	This app does not only work for images, but it also makes videos searchable while the competitor apps only work for images.

The SensifAI app is a bold move beyond the state-of-the-art compared to current image enhancement apps which require uploading contents into the cloud thereby exposing users to cyber threats. SensifAI works locally on the device, which protects user's privacy.

Besides, current image enhancement Apps only allow enhancement of images whereas SensifAI can also enhance videos.

Further extensions of SensifAI smart-enhance App also allows users to detect and blur peoples face or vehicles license plate in real-time. This feature helps users to be compliant with GDPR and avoid unwanted violation of other people's privacy while recording video in public areas such as museums, live- broadcasting or sharing image/videos in social media.

Making videos and images enhanced is a global challenge in the modern multimedia era where we are capturing and saving more and more videos and images every day. Image enhancement apps already have more than 50,000,000 users throughout the world. Although it creates a huge market, the real wave of users is yet to come, and the potential of the market is untapped due to fears of privacy violation. People do not want their images and videos transmitted to the cloud of big players before encrypting them. SensifAI yields a new smart-gallery app that makes images and videos enhanced with it performs all the processes locally on the NPUs and assures users full data preservation.

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

Testimonial

During the several coaching sessions, mentors had very interesting suggestions to maximise the impact of the project. SensifAI adopted the suggestions and applied the following advancements beyond the originally submitted and accepted proposal.

1) We developed the app for Smartphones with NPUs from Qualcomm and Huawei initially. However, according to the mentor's suggestion, we have also developed the app for any normal android phone which even has no NPU. Although the app works with less speed on smartphones without NPU, this implementation increases the impact and visibility and usage of the app.

2) Mentors suggested to release a public SDK such that if any other developer in the world needed image or video enhancement, they can directly use SensifAI SDK. SensifAI released an open platform to attract the contribution of other developers to use the results of this project.

   https://github.com/sensifai/Mobile_Image-Video_Enhancement

3) Mentors suggested adding a third mode beside superresolution and automatic enhancement such that users can manually use several tools and filters to modify their pictures. Therefore, we added the suggested filers to improve usability of the system and increase its impact.

Future plans

SensifAI plans to create a SuperApp offering many different image/video manipulation tools based on AI from different providers in one place and delivers it on both smartphones and PCs/laptops.

The planned App will include super-resolution, enhancement, cartoonizing, cut-out, summarization, background removal, face-conversion, avatarization, etc.

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

FAIR-AI: Designing human-centric AI to enable fairness assessments of texts

Summary

Fair Artificial Intelligence: Designing human centric AI to enable fairness assessments of texts.

Keywords

Fairness, Psychology, Machine Learning

Actors involved in the project

University of Cambridge:

- Dr Ahmed Izzidien
- Dr David Stillwell

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

The project

One of the pressing questions in contemporary AI, is how to make sure that its implementation is fair. Many methods have been suggested, with some more successful than others. In this project we wanted to take a step back and consider what was it that made an act fair, or unfair? Based on the answer to this, we asked, would it be possible for an AI to be able to detect what makes an act fair, or unfair? If one was able to answer this question, then potentially we could use an AI to assess situations for unfairness before they occurred.

This project began at the University of Cambridge, based on early research carried out by Dr Ahmed Izzidien when he was working at the Social Decision-Making Laboratory at the Department of Psychology. His interest was in finding the principal cognitions that humans used when making a fairness evaluation. This led him to a study of social preference games, such as the dictator game. In this game a person is given a sum of money, they are told they may give some, all, or none of this to a second person who is also taking part in the study. Contrary to early expectations by economists, they found the most people offered about 24 percent of the money.

Social psychologists like to do a lot of experimentation on human subjects and after an exhaustive iteration of alternative set-ups, e.g., using two related individuals, hiding one individual from the view of the other, etc., they found that one of the most telling factors that explained the giving, was the social responsibility score of the participant holding the money, and their perception of the situation as one that warrants such a sense of social responsibility.

The question then became, is it possible to program an AI to be able to detect and use 'social responsibility' as humans do?

Further research determined that a factor for the cognition of social responsibility was the ability to detect how the other person would feel if they were treated in a harmful manner. This is often referred to as the golden rule, and Rawlsian measure of justice when applied to society. That is, if I am willing to have the same act done to myself, then it is fair, and socially responsible.

To program this perception, Word Embeddings were used. These use vector representations of the concept of fairness – its social ontology. Based on this 'fairness vector' is became possible to measure how fair certain acts were, e.g., thank vs. murder. A paper was published from this study funded by the NGI Trust and can be found online https://link.springer.com/article/10.1007/s00146-021-01167-3, published by the Springer Nature Publishing Group, where one can read more about this project.

We will build on this for develop a 'fairness vector' to be able to read sentences and produce a score from -1 to +1 on how fair or unfair they are based on the metrics described in the paper.

In achieving this, it may be possible to design software that uses this perception, allowing AI to begin to detect those cues that humans use to class an act as fair, or not!

The completed project, funded by NGI Trust, was very well received by the staff at the university. The Cambridge Judge Business School mentioned it in its publications, as well as Hughes Hall college, of the University of Cambridge.

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

Testimonial

One of benefits found in working with NGI was that they maintain a good working relationship with the researchers. They provide useful coaching sessions, that allow for a lot of freedom and good technical and methodological advice.

The environment made by these sessions, and the NGI Trust in general, is very encouraging of new research, particularly on human aware technology. A theme that is becoming increasingly important as AI permeates into our shared social world.

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

MedIAM - Open source pilot implementation of secure medical IoT devices

Summary

According to cybercrime magazine, "healthcare suffers 2-3X more cyberattacks than the average amount for other industries", because the data has more value for hackers. Cyber regulations such as the EU cybersecurity act provide mandatory requirements to protect sensitive information and systems. Beyond traditional clinical systems of electronic health records (EHR), it remains really difficult to extend that line of requirements to connected devices people carry around as part of their treatments. If those medical devices aren't properly secured, people may unknowingly be broadcasting their health status, as well as many other personal sensitive data, everywhere they go. Or even be directly harmed by hacked devices. Existing protocols available for IoT are unable to meet the complete requirements from regulators.

In the current proposal, we provide an open source pilot implementation on how an equipment vendor should protect the functions and data of their medical IoT devices.

Keywords

Digital identity; IoT; healthcare; secure medical devices

Actors involved in the project

Fabien Imbault (lead), entrepreneur and founder of acert.io

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

The project

As a serial entrepreneur, working on the next opportunity is a peculiar moment. It's the time when you can reflect on past experiences, when you get to figure out where you might make a difference, and where your efforts will be focused on for the next 10 years. That preliminary research is a lot of hard work, from new ideas to technical prototyping. Our open source project being sponsored by NGI Trust was a fantastic possibility to discuss with our peers and disseminate those findings.

During the COVID-19 pandemic, digital platforms have helped keep the population safer, for instance via the remote tracking of chronic respiratory diseases or other comorbidities. This has led to an increase in the number of telehealth solutions and of medical devices being deployed in the field.

We started our project by analysing past security breaches. The results show that healthcare boasts one of the highest average rates of severe security findings. Not all types of healthcare organizations share the same struggles. Because they're still operating in closed legacy environments, hospitals are able to maintain their level of cyber hygiene, compared to ambulatory or nursing care facilities. In the current state of affairs, integrating with SaaS vendors or third-party connected medical equipment increases the risks, because most of them exhibit an inverted ratio for exposure relative to their internet surface area.

The industry should therefore put more emphasis on privacy-and-security-by-design as an integral part of their duty of care. And it will. Because public regulators, both in Europe and overseas, have acknowledged the vulnerability of those sensitive information systems and data, with new requirements taking the force of law.

Despite those well-established challenges, finding the right product-market fit has proven difficult. Our interviews with industry participants including CISOs, IT professionals, biomedical engineers, third-party vendors, healthcare professionals and patients, exposed a silo-ed approach to innovation. Most of the participants took improvement actions but had the feeling of institutional resistance from their other counterparts.

A way to reconcile those initiatives was to put medical efficiency at the centre. People didn't care much about network segmentation or machine identity, but were asking very pragmatic questions: what's our inventory of medical equipment? Are they well used and maintained? How can a remote maintenance process be integrated into the medical lifecycle and how would the various stakeholders - and the end-users in particular - be involved and benefit from it? How do you handle the large majority of devices that can't be updated?

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

The solution and the results

We designed various experiments to test our hypotheses.

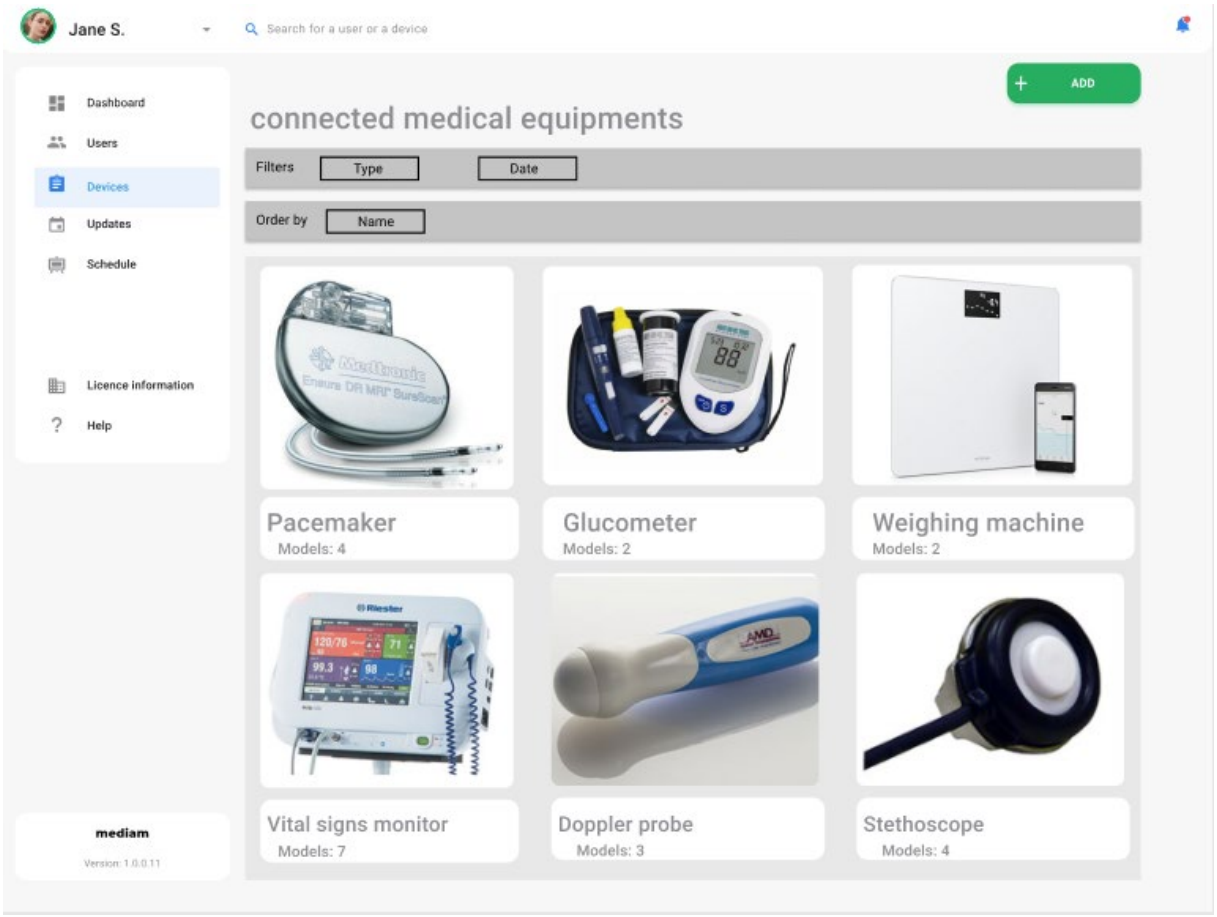


Figure 1. MedIAM prototypes

This had a profound impact on our technological choices. In particular, when implementing the security protocols, this helped us focus on a human-centric approach.

Apart from those field discoveries, the project followed its course as planned. We implemented minimum viable product experiments, got accepted two peer reviewed research articles, published some dissemination blog articles, updated an upcoming IETF standard and will be publishing a patent. We now plan to support those developments and broaden their scope into a new start-up that will focus on digital identity for privacy sensitive environments.

Testimonial

NGI Trust helped us a lot in our journey, as it offered great mentorship and advice from recognized experts, both on the technical and business perspectives. We also really appreciated the focus on how to build a business that builds upon an open source strategy.

Our project started in a less developed area, with the main objective of protecting children and young people using the Internet.

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

MidPrivacy - Identity Provenance as a first step towards personal data protection

Summary

Personal data protection is relatively new and often misunderstood, requiring to be looked at from a completely different perspective. Personal information cannot be handled as an ordinary data item. It is often crucial where the data comes from and what the overall circumstances of data processing are.

The solution is therefore based on the data and metadata - data about the data. When it comes to identity management and personal data protection, perhaps the most important part of the metadata is provenance information. That is why Evolveum's open source identity management and governance platform midPoint seems to be positioned at an ideal place in the personal data flows.

Work on the prototype took place in spring-summer 2020. The functionality enabled development of advanced personal data protection features, removing significant roadblocks. The provenance prototype was implemented as a part of midPrivacy initiative, a long-term effort to extend midPoint with a complete set of personal data protection features. After all, privacy and data protection are an integral part of midPoint design and day-to-day development.

Keywords

midPrivacy, midPoint, Axiom, identity provenance, data provenance, open source, identity management, identity governance, identity data, personal data protection

Actors involved in the project

Evolveum: https://evolveum.com

The project

MidPoint is the leading open source identity management and governance platform. With its rich feature set, this unconventional system gives organizations full control over identity data, making sure they are copied, synchronized and shared according to the policies. MidPoint is designed to improve information security, automate and improve error-prone activities, enabling organizations to proceed in digital transformation.

Figure 1. Evolveum

MidPoint is professional open source software, created and maintained by Evolveum. With its skilled full-time dedicated development team and valuable community, Evolveum works on maintaining and improving midPoint constantly. Due to the disruptive nature of open source software, a small company based in Slovakia is able to provide its services on a global market. This is no easy feat for a self-funded company with less than 30 employees and a product that is completely open source. That is why an efficient partner network and empowered user community are instrumental in addressing customers' needs all around the world.

The problem

In early days of identity management, the technology was all about cost saving and information security policies. Later on, the focus shifted to identity governance and management of compliance with laws and regulations. While these concerns are undoubtedly important, there is one concern that is unique: personal data protection.

Personal data protection is a special concept in many ways. First of all, it is relatively new and often misunderstood. There are numerous attempts to address personal data protection with existing information security tools, governance and compliance frameworks. However, these attempts are rarely successful, as such tools are lacking the appropriate mechanisms. Personal data protection is not about "can user X access system Y?". We need to look at the problem from a completely different perspective. Personal data protection is mostly about "can we process data A for the purpose B, given circumstances C?". This question is much harder than it seems, and the systems that can efficiently answer such questions are extremely rare.

The core of the problem is in the data, or rather the fact that data are not just data. Traditional systems handle user's full name as an ordinary data item. They use it and share it without any considerable limitation across the entire organization, and even beyond organizational boundaries. However, personal information cannot be handled as an ordinary data item. It is often crucial where the data came from and what the overall circumstances of data processing are. For example, if user is an employee of our organization, we are entitled to keep this information and use it within our organization

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

as necessary. However, when an employee leaves, the situation is much different. We might still be able (and even required) to keep the name of the user. Yet we are no longer entitled to store it and use it in numerous information systems in our organization. The data item is still the same, it is still stored in the same database, however, the circumstances are all different. Appropriate data minimization and erasure has to take place.

This is still a very simple scenario. We are living in a connected world. The boundaries between employees, partners, customers, students and community are very fuzzy. How can we process user's full name, if the user is a student, they are engaged in two research projects, each of them spanning several academic organizations? How does the situation change when the student graduates and becomes employee of one of the partner organizations, still participating in one of the projects? These questions are not easy to answer.

The solution

The problem has a surprisingly complex and multi-faceted solution. The solution is based on the data - and metadata, which are the data about the data. We need to know a lot of details about user's full name: where it came from, when we have first learned about it, when it was updated for the last time, how it was created from the first name and last name. When it comes to identity management and personal data protection, perhaps the most important part of the metadata is provenance information. Provenance tells us where the data came from, which in turn determines how we can use the data. Once again, provenance is more complicated than it seems, as a data item may come from several overlapping sources, or it may even be a combination of several values.

MidPoint development team had been aware of the problem for several years. The team has an outline of a solution, as midPoint seems to be positioned at an ideal place in the personal data flows. However, when it comes to practical solution, the problem goes deeper than the technology. Personal data protection is based on fundamental mechanisms, such as auditing for accountability, integration components for data transfer, policies and so on. MidPoint already has most of that mechanisms. However, one crucial piece of the puzzle was missing: data provenance.

Provenance metadata are not simple, as we have seen. Data provenance is also a problem that is not understood completely. Therefore, there is a need for a complex metadata schema support in the data representation layers. Metadata schemas must be easy to adapt and extend, otherwise the solution would be too limited for practical use. However, none of the popular data modelling frameworks have such support. Simply speaking, there is a lot of groundwork to do, before first practical benefits for users can be done. While the final product features are likely to be commercially viable, the foundation work is a considerable barrier.

Evolveum had been trying to secure funding for the metadata groundwork for years, until an opportunity was provided by NGI_TRUST. NGI_TRUST provided funding to build a personal data provenance prototype to lie the foundations and demonstrate feasibility of the technology.

Work on the prototype was done in spring-summer 2020. The objective was a demonstration the feasibility of complex data provenance metadata in a practical and established identity management system. The code is an evolutionary prototype, which is

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

a native part of midPoint source code, continually improved during regular midPoint development cycles. Modelling of complex metadata structures proved to be a major challenge, which was quite expected. The challenge was addressed by designing and developing Axiom, a new data modelling language with native support for metadata modelling. Axiom was a success; its capabilities were proven several times during the project. The flexibility of Axiom was a real benefit, as metadata schemas changed dramatically several times during the project. The team has encountered unforeseen difficulties, caused by limited experience of identity management community with data provenance metadata concepts.

Results

Despite the difficulties, there is a complete working prototype at the end of the project. The prototype has demonstrated the ability to attach complex provenance metadata to any individual value in the identity management system. MidPoint knows where every value came from, even in case it came from several independent sources. The metadata are processed together with the value. For example, when user's full name is computed from first name and last name, the resulting full name value will reflect provenance metadata from the first name and last name values.

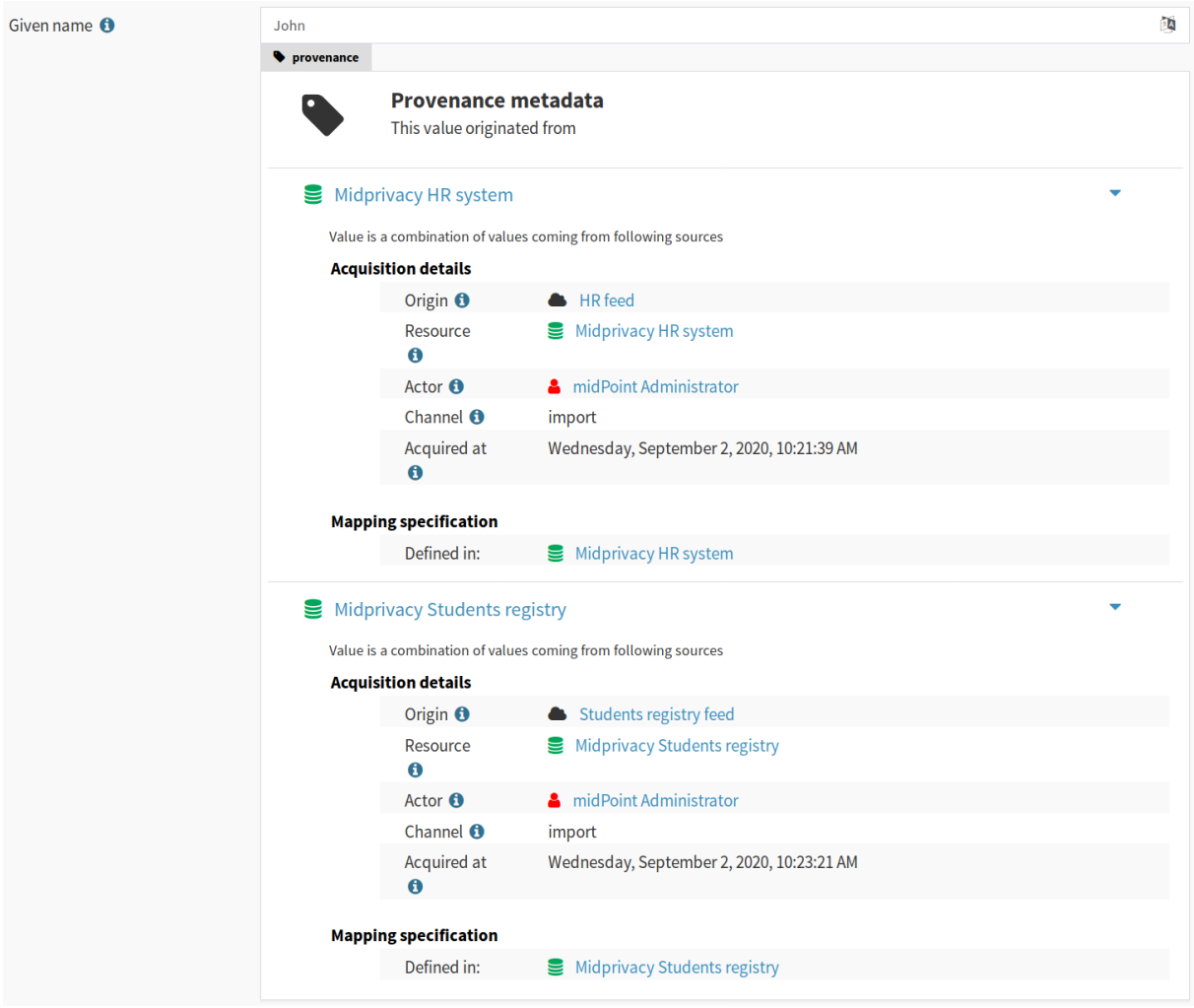


Figure 2. MidPrivacy prototype GUI

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

MidPoint user interface is metadata-aware, it is able to display provenance information for all the values. Axiom, the metadata-native modeling language, shows a great potential for further development and practical use by a broad community. Overall, the prototype has reached and exceeded the expectations.

Testimonial

The help from NGI_TRUST was an essential part of the success. NGI provided the funding, yet the guidance and coaching were also very helpful. This is one-of-kind opportunity, an impulse without which the functionality might never get developed.

Future plans

Being a prototype, the functionality is still in a nascent stage, yet it shows a commercial potential. This functionality enabled development of advanced personal data protection features, removing significant roadblocks. With the prototype in place, further development of production-ready functionality becomes commercially-viable.

Unfortunately, further development of the functionality was slowed down by the events related to the pandemic. The customers have shifted their priorities towards more pressing concerns, displacing personal data protection. However, we believe that the interest will be revived as the economy recovers. We already have preliminary plans to continue development of both Axiom and the provenance functionality.

The provenance prototype was implemented as a part of midPrivacy initiative, a long-term effort to extend midPoint with a complete set of personal data protection features. Privacy and data protection is not just an after-though in the midPoint world, it is an integral part of midPoint design and day-to-day development. After all, personal data protection is not just a legal requirement, it is the right thing to do.

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

SensioID: Solving ownership and copyright for the digital creative market

Summary

Kelp.Digital (ex. Sensio) is open-source software for content creators (for now, mainly, photographers) to manage, protect and license their work. Simple, transparent and secure.

In the long run, Kelp's goal is to form a creative market where content creators are not bound to any platform and can set the terms for others to use their work without much effort, and where publishers, marketers and other creatives can acquire quality content directly from its authors in a few clicks.

As the first step towards this ambitious goal, within the scope of NGI_Trust, we have developed a tool that will help photographers to stay in charge of their work while publishing and sharing photos online.

Keywords

Copyright, blockchain, substrate, digital identity, creative market, content creators, photography

Actors involved in the project

Daniel Maricic (7Signals.io), Elena Tairova (Sensio.Group)

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

The business

At Kelp.Digital we build open-source software for content creators (for now, mainly, photographers) to manage, protect and license their work. Simple, transparent and secure.

It all started as a relatively small project to fix issues in one photographer's workflow: back in 2017, Daniel [Maricic] started working on a simple yet elegant solution to improve his own workflow when developing and sharing photos. However, the project's scope and ambition quickly expanded. The more we looked in the market of digital photography and talked with the content creators, the more the issues in the field became obvious.

In 2019 the project idea took its current shape and both Daniel and I [Elena Tairova] decided to dedicate our full-time to making the market of digital photography more open, transparent, and fair towards the content creators.

Daniel Maricic (7Signals.io), Elena Tairova (Sensio.Group)

Our first step towards this ambitious goal was to develop a tool that would help photographers to stay in charge of their work while publishing and sharing photos online. We had a proof-of-concept and the first prototype ready when we applied to NGI_Trust 2nd call with our proposal.

The problem

So, what exactly is wrong with the market of creative content today? Quite a few things actually, but to put it shortly: the field is highly centralized, unfair to the content creators and, as a result, underperforming.

If you think of it, practically every internet user today is a creator of digital content: thousands of photos and videos published by an average user every year. At the same time, the majority of content distribution and management lies in the hands of very few tech corporations who impose their terms. Creators, in fact, have very little control over images and videos they share online. Once published, the content is often detached from the creator. It can be copied without attribution and used without author's consent. Talented people miss out on their fair reward, but that's not the only issue. Stolen images can be misused in identity thefts, blackmailing, or spreading misinformation.

The market of creative content as it is today doesn't work quite well. The recent approval of the new EU Copyright Directive and a contentious debate about its Article 17 (previously

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

art.13) makes it apparent. However, addressing the copyright issue by filtering and upload prevention is hardly a solution in itself.

The solution

At Kelp, we believe that the key to resolving the creative content market issues is not through fighting the industry incumbents. Instead, we are working to kick-start the transformation from within: from the users, creators of the content.

First and foremost, to truly put users in charge of the content we need to provide an easy-to-use content management tool with built-in copyright protection, fast & secure licensing and copyright transfer. The idea is to simplify the workflow: from organizing collections to sharing and managing on external platforms, and to, ultimately, selling or transferring the rights.

By putting a user in the centre of the system, we will prevent data locking, improve connectivity with different providers and create a more transparent and secure ecosystem.

To test our idea on the market, we decided to start with professional photographers and video makers, who we see as our first adopters and ambassadors. Being knowledgeable about the market and struggling with its bottlenecks and unfairness on a daily basis, these users are in need of a better tool to simplify their workflow (and their lives).

Within the 9 months of NGI_Trust project (April-December 2020) our goal was to design and build a web application for professional photographers that would allow them to create legally valid and verifiable digital copyright statements for their work in a simple and straightforward way. Yet, to enable the above, first, we needed to create a robust algorithm for copyright storage validation and creation.

The other projects aiming to tackle this issue essentially offering Proof-of-Existence statements created by time-stamping services. They confirm only the fact that a certain digital asset existed at a certain point in time providing no evidence whatsoever about whether a user uploading the content is a creator and a rightful owner.

Our approach is different. Before anyone can claim copyright of a photo a user needs to go through the equipment/device verification workflow. Therefore, ownership of a physical asset needs to be proved first. Only when that is in place, a user can claim copyright of the photos created with that equipment.

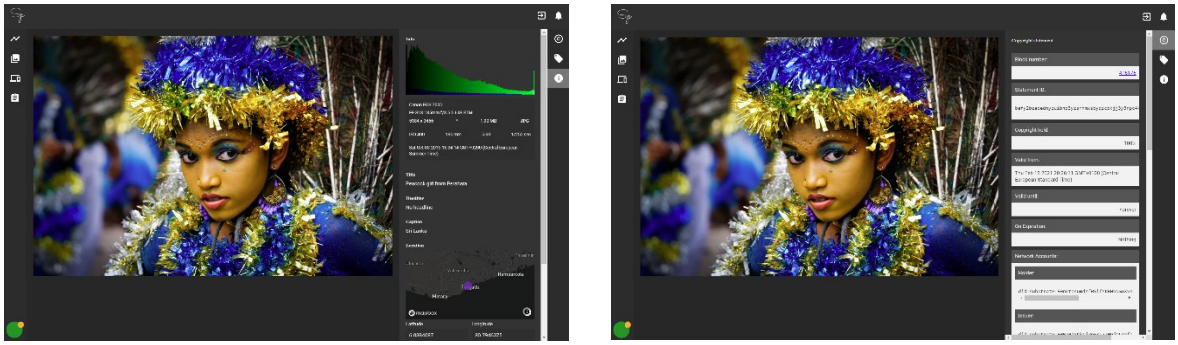
If successfully scaled, Kelp.Digital solution has the potential to become a key infrastructure for the new transparent market of creative content in the human-centric internet.

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

Results

Throughout the implementation stage the project's initial concept expanded significantly and ultimately grew into Anagolay.Network, a decentralized protocol built on Substrate framework that allows multimedia content creators to sign, permanently record, and create statements about their copyright and ownership.

On top of the Anagolay, we built a web-application for digital photographers, currently available under private Beta and developing into Kelp.Digital. The app has an integration with Lightroom CC that allows photographers to sync their albums. A straightforward equipment verification process allows photographers to claim ownership of camera & lens combination. Once the equipment is successfully verified a user can generate copyright statements for all the photos taken with the equipment they own.



Interface of the private beta version of the web app and Copyright statement details

Throughout the project implementation, we have been not only testing our solution with the photographers but also making sure it is valid from the legal point of view. Through our partnership with the Blockchain School for management and collaboration on the "Legal applications of Blockchain & Compliance" programme, we established that digital statements created by Kelp.Digital are legally binding and can be used as sufficient evidence in court.

Testimonial

Back in 2019, we took part in the NGI Community event in Helsinki while looking for funding opportunities to keep working on the project, which initially was financed from our personal savings. Among various projects under the Next Generation Internet Initiative umbrella, NGI_Trust seemed to be a perfect fit.

The application process was pretty straightforward, even though it was our very first time applying for a grant. In about three months' time we got the exciting news about our proposal being selected under the 2nd open call.

First and foremost, NGI_Trust funding allowed us to keep working on the project full time and allocate additional resources to move faster. Besides, given the complexity of the project, doing additional research and testing new ideas had become our long-time habit. Having a set framework and a fixed timeline helped us to stay focused and move faster.

The three coaching sessions spread throughout the 9 months' timeline proved to be particularly useful, as they motivated us to ship feasible and coherent results in time for every session in order to make the most from our conversation with our coaches. Additional IP consultations were a nice addition - they gave us a nudge towards getting stronger trademark protection.

Overall, the straightforward communication and minimal amount of paperwork required by NGI_Trust allowed us to concentrate efforts on the project implementation and work in our full capacity.

It's also worth mentioning an additional perk that came with being a part of NGI community - our participation in Tetra Bootcamp. As one of the Pitching Competition winners, we got additional business mentoring support which we keep benefitting from.

If like us, you are working on a project with an aim of making the Internet more transparent and a safe place for the users, the resources that the NGI initiative has to offer can be of tremendous help.

Future plans

In the long run, Kelp's goal is to form a creative market where content creators are not bound to any platform and can set the terms for others to use their work without much effort. Where publishers, marketers and other creatives can acquire quality content directly from its authors in a few clicks.

We still have a long way to go before we get there. Our primary focus for 2021 is to keep working on Anagolay.Network to make it stable and production-ready. Along with improving the network capabilities, we will gradually move towards the decentralization of the platform. The idea is that with time any trusted entity on the Network can become an 'Issuer' - a trustee signing the copyright & ownership statements on the Network.

The web application which is currently available under private Beta, will be open to the wider community in the next few months under the new name Kelp.Digital. The name choice, of course, is not random. The underwater Kelp forests are known to protect all its

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

inhabitants: from whales to the smallest fish. That's exactly what the digital Kelp will do - protect all the content creators and their work in the Internet waters.

Throughout 2021 we will keep improving the Kelp web app based on the feedback received from our first testers, and work on the new features, prioritizing based on the community requests.

The next step will be launching a mobile application which is the key to scale-up and onboard a broad audience of casual smart-phone photographers & bloggers.

Ultimately, in 2 years from now, with Anagolay.Network battle-tested and with content creators actively using Kelp.Digital to protect their work, we will be ready to launch the Peer-2-Peer marketplace for digital photography & videos.

As you can see, we have pretty ambitious plans and NGI_Trust allowed us to get started. If you want to join us or learn more visit:

Sensio.Group: https://www.sensio.group

Kelp.Digital: https://kelp.digital/

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