Funded Projects Call 1

Project Number	Proposal Acronym	Lead Partner (name)	Partners	Keywords	Abstract
92	ISIBUD https://www.betterinternetsearch.com/	Better Internet Search Ltd, **UK** Project lead: Gordon Povey	Edinburgh Napier University	browsing, user-centric, machine-learning, privacy	There has been growing dissatisfaction with incumbent search engines and their use of our personal data for targeting advertising. An alternative user-focused business model will be tested with real users during this project to prove not only the technical viability but also the commercial viability of the new user-focused models. This project will deliver a demonstrator to show that internet search can be significantly improved by adopting a user-focused model for both the ranking of results and for the monetisation of the search engine itself. The project team has already developed an ad-free organic search engine and in this project supervised machine-learning is applied to improve the ranking and personalisation of results while fully respecting the privacy of the user by keeping all personal data on the user-side and under the control of the user.
15	Decentralize messaging https://danubetech.com/technologies.html	Danube Tech GmbH, **Austria** Project lead: Markus Sabadello and Dominik Beron		SSI, open-source, user-control, decentralise, messaging app	A small number of organizations manage most online interactions/communication leading to known centralization issues (e.g. data silos, privacy scandals, massive security breaches). Also, online fraud (e.g.ID theft caused by phishing) is creating billions in damages. Solution (Project): To create a human-centric internet we need to decentralize the way people interact online and give them control over their data and digital identities. To realize this, the project will develop "Context", a novel type of application that is decentralized on all architectural layers and can utilize SSI, i.e. an open, universal and extensible identity infrastructure. Context will be the first messaging uApp and will deal with the follow issues: • Value(Users): Context enables people to interact/transact directly (P2P; without intermediary), gives them full control over data (incl. portability) and enhances security (e.g.private key encryption, signatures, key management) and privacy (e.g.minimal /selective disclosure via zero-knowledge-proofs). Fraud (e.g.spam, phishing) can be prevented and trust established without a central authority (e.g. platform). Thus, Context will be an alternative to centralized messengers (including e-mail) and potentially for platforms in different verticals. • Value (Ecosystem): Context would establish a framework/best practice for developing uApps. Apart from open sourcing(at least the core) code of Context, the project will provide additional OSS (Apache 2) that facilitates uApp development for others.
22	INSTANT https://www.virtualangle.com/instant-project/ @Virtual_Angle @pmlbranco	Virtual Angle BV, **Netherlands** Project lead: Pedro Branco		user-control, portal, big data	In 2011 the World Economic Forum(WEF) issued a report stating that 15 billion devices will be connected to the internet by 2015 and 50bn by 2020. The amount of data stored on the internet is predicted to grow exponentially and looks set to be 44 times larger in 2020 than it was in 2009. Global internet services revenue has also grown strongly over the last ten years, and is forecasted to reach 554 billion Euros in 2019. Internet giants have business models underlined by the use of personal data, but most people would have trouble knowing who exactly has access to their personal data, for what it is being used for and what benefits it's generating for the enterprises that are using it. Artificial Intelligence and Big Data technologies potentiate an increasing number of personal data applications. Advertisement, Medical, Banking and Media industries are profiting while using individual's personal data while not delivering adequate compensation to each individual.It's urgent to increase transparency regarding the usage of personnel data by enterprises and to ensure that users are better compensated for providing others with access to their personal data. INSTANT aims to empower users with a transparent tool to manage the access to their personal data and to support due compensation by its use by third parties.INSTANT is focused in delivering a common interface where users will be able to: store the information of each organisation to whom they delivered personal information; create, edit and revoke personal data access given to each specific organisation; manage potential financial compensations given by each organisation for using the user's personal data. INSTANT will deliver an online portal, and an associated set of web services and protocols, which will serve as interface towards individuals and the data industry.
41	MyPCH https://mypch.github.io/	Diabetes Service ApS, **Denmark** Project lead: Jan Leindals	OwnYourData, **Austria**	privacy, sensitive data, self-monitoring, open source	There are 425 million adult people (1 out of 11) diagnosed with Diabetes in the world today and it is a growing epidemic. The diabetes treatment is a very complex puzzle to get the right dose of medicine and many people do not have adequate resources to follow the prescribed dose regimes. This leads to serious healthcare issues and increased costs. The good news is that technology like self-monitoring devices of blood glucose can help solve the dose puzzle by using a data-driven diabetes management approach. Sharing these new digital health data from self-monitoring devices with doctors, researchers and others is indispensable for success. We believe that our innovation is a paradigm shift in sharing self-monitoring health data. The innovation will be open source, empower the individual by sharing data in a secure, trusted, auditable, traceable and consensus-based way inspired by MyData principles. MyPCH presents a standardized way to exchange health data in a privacy- respecting data flow between various stakeholders in use cases, so the user can: • Collect data from medical devices using a PC and store it into a Semantic Container. A Semantic Container packages structured and semi-structured data, semantic description of the data (ontological characterization of the data, usage policy, provenance), and processing capabilities into a single container. All data is made immutable by storing a corresponding digital fingerprint using blockchain technology. • Save, manage and visualize data in a self-determined way in a personal data store to derive unbiased insight. • Share data with others by uploading data to a public cloud service with a semantic container. Sharing can be either personal identifiable information with clinics and aggregated anonymous data with researchers.

79	TCN	Athena Research and Innovation Center in Information, Communication and Knowledge Technologies, **Greece** Project lead: Vassilis Tsaoussidis	University College London, UK	decentralised, DLT, reputation	The Internet, initially designed as a distributed system, has become increasingly centralized in recent years and relies on centralized mechanisms to support its core functions, such as trust . At the same time content, although largely created by, and exchanged among users at the edges of the network, is stored on commercial, centralized, services. This project focuses on assessing the feasibility of deploying a decentralized, reputation -based trust mechanism to solve security and trust problems in Named Data Networking , a future Internet architecture. We consider two use-cases: In the first one, we provide a lightweight mechanism to validate content authenticity in the intermediate routers to mitigate cache poisoning attacks, a serious security threat in NDN. In the second one, we consider trust ratings to be tied to content quality, assessing the feasibility of deploying such a mechanism at the network layer to prevent malevolent content (e.g. fake news) from spreading in the network. To decentralize our trust scheme and eliminate single-point s of failure, TCN will leverage the blockchain paradigm. Furthermore, we utilize the Proof-of-Prestige consensus algorithm to bring our platform closer to real-world deployment, by inducing an incentives and reward s system for users to provide their ratings and assess its effectiveness.
63	CryRev https://cryptech.is/	Assured AB, **Sweden** Project lead: Joachim Strömbergson		HSM, cryptography, key management	Working since 2014 the CrypTech project (https://cryptech.is/) has developed an open-source hardware cryptographic engine design to meet the needs of high assurance Internet infrastructure systems that use cryptography. Our open-source hardware designs are aimed to be of general use to the broad Internet community, covering needs such as securing email, web, DNSSEC, PKIs, etc. The project has produced a design and hardware boards that have been used in various experiments and tests. Our current alpha-board is now being productised by a not-for-profit US company (DiamondKey). The current design has been the subject of a positive external security evaluation (https://cryptech.is/2018/10/external-security-audit-completed/), though of course some possible improvements were identified in that process that are being or have been addressed. NGI-Trust funding will fund the Cryptech core team in designing and prototyping our next revision Cryptech designs/board.
11	CAP-A A Community-driven Approach to Privacy Awareness Twitter: https://twitter.com/CapriceSociety https://www.venafi.com/blog/fighting-privacy-fundamental-human-right-war-encryption	FORTH, **Greece** project lead: Giorgos Flouris	IN2	consent, privacy, terms of service,	In an increasingly instrumented and inter-connected digital world, citizens generate vast amounts of data, much of it being valuable and a significant part of it being personal. However, controlling who can collect it, limiting what they can do with it, and determining how best to protect it, remain deeply undecided issues. CAP-A will deploy a socio-technical solution based on collective awareness and informed consent, where by data collection and use by digital products are driven by the expectations and needs of the consumers themselves, through a collaborative participatory process and the configuration of collective privacy norms. The proposed solution will create a new innovation model that will complement existing top-down approaches to data protection, which mainly rely on technical or legal provisions. The project will deliver a global repository of consumer-and developer-generated content about the privacy behaviour of digital products, along with tools that will help consumers understand the Terms of Service and their implications via crowdsourced approaches and visual cues. The objective is to foster collective intelligence and co-creation of solutions, and to facilitate the participation of all involved stakeholders through an open architecture, thereby allowing novel uses of the privacy-related content. Ultimately, the CAP-A ecosystem that will be formed will strengthen the trust bond between service developers and users, encouraging innovation and empowering the individuals to promote their privacy expectations as a quantifiable, community-generated request.
34	PY Protect Yourself https://twitter.com/PangaFR	PANGA, **France**	MyDataBall, **France**	IoT, data privacy, big data, consent, SSI	Since the democratization of Internet, new businesses have been emerging, leading to the explosion of e-commerce market places and the IoT which is providing many connected devices and solutions for all business sectors(healthcare, automatic domestic equipment, automotive industry, etc.). Data privacy is thus becoming more and more challenging as people are giving their personal data to big companies (likeGAFAMI), inadvertently, or without being quickly and visually aware of the risks, or just because of lack of protection solutions. The PY box is the central check point for all your connected devices. This complete hardware and software solution aim at informing and protecting citizens from the unknown connections and unwanted data flows that automatically start when a device is connected to internet. Thanks to a user-friendly interface, the system graphically shows the status of all the activities, provides risks assessment and allows you to define your personal security settings and your authorized personal data. PY platforms will protect you without fear of degrading the functionality of your devices. On the contrary, the speed of use will be improved by reducing unnecessary connections or messages. The AI module will serve your interests while preserving you from the undesirable. Addressed challenges:The digital identity protection, through the creation of dynamic and volatile digital avatars thanks to SSO systems in order to avoid the calculation of metadata, the trace ability of the activity, the use of uniqueID and password for several websites. The protection of local network, by implementing solutions that are developed on purpose: Firewall, IPS and anti-virus that are integrated on a unique platform. The growth of awareness of risks related to IoT, PC and smartphone data, by warning the users about the possible threats and by performing risks analysis that can be viewed on a user-friendly interface.
78	EUACTIVe Educate, Understand: Act, Control, Trust & Value your Data when going online. A dynamic VPN by design (as an API) & a Personal Data Passport including Portrait-Right; For All!	VDP, **Netherlands** Project lead: Laurent Engel	NHL Stenden University of Applied Science TÜV Rheinland ilionx	DLT, app, privacy, user centric	Imagine a world where all individuals have control over their personal data. No data lost or stolen, full control and ownership in the online spectrum. That's a friendly & trustworthy system. ValueMe is creating this ecosystem. A C2B principle, individuals in control, aiming at safer, relevant and more trustable online journeys & relationships. ValueMe noticed; "current online activities are poisoned by advertising models creating waste, irrelevance, less trust". Founders Henri and Laurent Engel and their team conducted multiple studies, showing Advertisers spending more on online marketing budgets but see lower ROI and their "targets", the consumers, see less relevant offers-advertisements or info. Why? Because the current model has turned the individual into a product. Advertisers shoot hail and consumers have no voice or option saying "Listen to me! This is who I am, this is what I like and need!" The ValueMe ecosystem is consumer-centric, giving every human being the possibility to share, own and control their personal data.
55	COP-MODE Context-aware Privacy Protection for Mobile Devices https://cop-mode.dei.uc.pt/	Joao P. Vilela, **Portugal**	Alastair Beresford, UK	privacy, mobile, user centric	The main goal of the COP-MODE project is to advance the state-of-the art on privacy protection mechanisms for mobile devices operating in ubiquitous computing environments. The pervasiveness of mobile devices (e.g. smartphones) allows great quantities of data to be collected at all times. This collection can be beneficial for both users and collecting entities, by facilitating user-tailored services. However, much of this data can also be considered private and sensitive, thus requiring privacy protection mechanisms that can provide an adequate trade-off between utility and privacy. Current systems fail to provide adequate privacy protection by relying on an ask-once use-every-time approach, in which mobile applications ask for access to certain types of information at install, and have access to that information at all times without user intervention. Warning users of privacy risks has proven ineffective due to warning fatigue, in which users gradually dismiss messages that become annoying or intrusive, especially when users have dozens of applications, each with several privacy-related preferences to set. Moreover, some studies have shown that there is an inherent context-dependence of privacy decisions; however context is challenging to model and define. In this project we plan to address some of these challenges, in particular we plan to gather the necessary data for developing privacy profiles that map privacy preferences with context. These datasets and privacy profiles shall form the basis for future development of automated mechanisms for setting privacy preferences on behalf of users according to current context.

80	Edge-TINC Decentralised Edge Gateways for Trusted In-Network Computing	Fluentic Networks Ltd, **UK** Project lead: Dirk Kutscher		cloud, IoT, decentralised, network stack, DLT	The traditional, centralized cloud computing model in use today has difficulty handling new and emerging applications and networking paradigms. As user and IoT devices are becoming ever more powerful, they are producing enormous amounts of data, for safety (street cameras), entertainment (UGC and AR/VR applications), health monitoring (wearable devices) and intelligent transport applications (autonomous vehicles). Pulling this data into the cloud for processing is impossible due to the enormous volume, but also due to stringent latency requirements. Instead, in-network and edge-network devices will collectively form edge computing swarms and complement the cloud with their data storage and processing resources. This shift from centralized to in-network compute has the potential to open up new horizons for application development, ultimately, creating new markets for storage and processing resources. As a first step towards the bigger vision, Edge-TINC will design and implement a proof-of-concept prototype of an edge-network gateway (implemented in Rasbperry PIs, WiFi Access points, or similar) that implement the first generation of In-Network Computing protocols.
48	DECIDE DECentralized Identity and User Experience https://www.ngi.eu/blog/2020/02/26/whos-ngi-alina-khayretdinova-making-decentralised-identities-easy-to-use/	University of Stuttgart (USTUTT), **Germany** Project lead: Stephanie Weinhardt		decentralised, SSI, DLT, privacy	Decentralized identities (DIDs), also referred to as Self Sovereign Identities (SSI), are a novel promising approach to Identity Management (IdM) based on the Blockchain technology and a Privacy Enhancing Technology (PET). Numerous companies and projects whether big or small, are currently working to make this approach a product for trustworthy and privacy friendly identification in digital interactions. Their technical architecture and proofs of concept show that it is possible to realize such Blockchain- based IdM solutions. This promises to lead the way for a new area of PETs , which would lead to a trustworthy and privacy-friendly internet. However, experience shows that although PETs are a major building block for ensuring privacy on the internet and even though they have a high technical functionality and security, user adoption and diffusion of secure and privacy friendly IdM and similar technologies are not as high as they could be. Currently, development of PETs focuses mainly on the technical feasibility and implementation. Usability for end users and service providers' requirements are often neglected. Thus, the technology is often very secure and privacy friendly but lacks applicability in practice. This leads to users not adopting PETs as well as they could be, resulting in security or privacy inci- dents. Moreover, the (business) potential of PETs is not fully exploited, as they are not attractive enough to service providers and therefore rarely integrated into services. Therefore, DECIDE will conduct a prototype-based study, analysing and evaluating the DID technologies currently in development towards their practical applicability for end users and service providers. Based on the findings the project will develop further (a) user friendly prototype(s) of a DID wallet to enable users to make informed decisions considering security, privacy and trust and thus establishing trust and privacy relationships with other users or services. Moreover, it will (b) derive recommendations making DID technologies valuable for service providers in their business processes. Project results will help the actual diffusion of privacy enhancing technologies in the context of identity management that enable trusted interactions in the digital sphere.
66	D4S Design 4 Security - Making VPNs Easy https://www.eduvpn.org/ https://www.letsconnect-vpn.org/	DTU, **Denmark** Project Lead: Tangui Coulouarn	KADK Commons Caretakers	VPN, privacy, identity, user friendly	Let's Connect! provides an open source secure VPN solution allowing ISPs, hosters and businesses to easily setup a secure VPN service. After deployment, users have a safe path either to their company or to the Internet from all generic devices. What makes Let's Connect! unique in respect to other VPN solutions? Let's Connect! is the only Open Source solution that has released both server-side management software as all clients apps. The other key strengths of Let's Connect! come from the focus on security and strong cryptography; the integration with existing Identity Management Systems ; the focus on privacy and GDPR compliance. The project is known under two names: Let's Connect! and eduVPN. The brand eduVPN is used to promote this VPN solution to international educational and research organizations. Let's Connect! has been supported by GÉANT project, RIPE community fund, SIDN fund (.nl registry), Vietsch Foundation and the NREN community. Led by the Technical University of Denmark (DTU), D4S aims to reinforce a specific aspect of Let's Connect!: user experience. The goal of D4S is to help solve a well-documented issue met by many security solutions: even if when they are aware that security is important, end-users don't necessarily use security solutions because they have a cost. There will be three main components in the project: a design process coordinated by the Royal Danish Academy of Fine Arts and an implementation component led by the Commons Caretakers - which has been leading the development of Let's Connect! for several years in collaboration with the Commons Conservancy and which works regularly with developers. A third component will consist of the development of a full Linux app.
86	CASPER Twitter : https://twitter.com/CASPER_NGITRUST	School of Electrical Engineering (ETF), **Serbia** Project lead: Prof Aleksandar Jevremovi	O Mundo da Carolina - Associação de Apoio Crianças e Jovens Faculty of Computer Science and Engineering, "Ss. Cyril and Methodius" University, Skopje (KINKI)	sensitive data, privacy, protection, AI	As children are a particularly sensitive category, next generation Internet should be designed in such a way to protect them from both general (untargeted) threats and threats based on user profiling. Current way of user profiling and data collection strategies are particularly dangerous for them - as even adult individuals need help to make more informed decisions on the relevance of information that they are asked to disclose when accessing and using services. Thus it is not surprising that nowadays there are many solutions related to children protection on the Internet. These solutions are using the different approaches, in order to prevent child to access inappropriate contents (e.g. pornography) IP filtering (e.g. OpenDNS by Cisco) is used, search results are limited (e.g. SafeSearch by Google) or image and texts are analyzed by parental control software (e.g. Norton Family Premier). However, these solutions are not 100% effective - e.g. some domains/IP addresses are still not in the databases (and the adding process could be very slow), some regular sites get hacked, some sites are XSS vulnerable, content-sharing networks can include harmful content, some content is encoded in a specific way, etc. The approach we propose within this project, instead on checking source reliability, is focused on the content presentation. It means that we are focused on using A.I. methods to check if the presented content (textual, audio or video) is appropriate for being shown to a child. The proposed approach could be considered as an ultimate solution for two reasons. Firstly, it is focused on the final HCI layer, where all underlying components and technologies are aggregated. Secondly, it is based on A.I. simulating human perception, that strives to provide the most human-like decision.
94	CCS Cozy Cloud's Shiffremir @cozycloud https://cozy.io/en/	Cozy Cloud, **France** Project lead: Paul Tran-Van		privacy, personal data, encryption, user control	Today's internet most successful platforms (Google, Facebook, etc.) not only neglect users' privacy but base their business model on personal data brokering. Indeed, over the past decade, personal data has become the new gold across all sectors. At the same time, repeated scandals resulting from personal data leaks led to awareness raising over the past years1,2. Furthermore, in Europe, the GDPR now protects users against data misuse. Consequently, privacy has become both one of the main challenges and an extremely valuable criterion of the next generation internet services. Cozy is a French start-up that has developed an open-source cloud platform protecting your personal data. Our ambition is to reverse the established order to empower internet users as we provide them their own "digital home" and give them back the control of their data. We already dedicated over 6 years of research to our project and want to go further to fulfil our initial goal and commitments. As one of the most powerful leverage for a real privacy enforcement, the Cozy Cloud's Shiffremir (CCS) project focuses on data encryption. This project overall objectives are (1) to exempt the end-user from trusting any service provider back-end, including Cozy Cloud, and (2) to ensure that our system is usable by any non-technical user. This project technical objectives aim to overcome the major bottlenecks (performances, feature loss and sustainability) involved by this new paradigm.
99	b-smart https://things.is/	THINGS, **Italy** Project lead: Pier Bardoni		IoT, licensing, user privacy	One of the main issues related to the upcoming vision of the IoT is related to privacy: in particular, setting privacy controls. Nowadays, we tend to go through software licences without reading them, as they are too complex, too long, and written in legal jargon: usually we get to the end and press "I agree" without reading a single word. With the advent of a large number of connected objects, able to sense our environment, it is of fundamental importance to give to all users means to control the privacy settings. Furthermore, it would be very relevant to propagate them to semantically similar devices. On top of it, several connected objects may not even have displays (or just very basic ones), making this task even more difficult. The objectives of this study are therefore three: on the front side, develop a human-centric interface, providing the best User Experience for managing privacy settings; on the back side, an architecture, including design patterns and interfaces and algorithms to propagate them and transport them between different providers and objects; on the "far away" side, how to make the above-mentioned work meaningful and a long-term success.
70	Keyn https://keyn.app/ @KeynApp	Keyn B.V., **Netherlands** Project lead: Wouter Segijn		authentication, apps, browser extension, encryption, decentralisation, software dev	Password authentication has been the primary means of authentication for web applications since the early days of the Internet, but suffers from both security and usability issues. We are developing a solution that allows people to log in to websites more easily and more securely using their smartphone. It bridges the gap from password authentication to strong authentication on the web, by creating a uniform user experience for a variety of existing authentication methods. The solution consists of a smartphone application and browser extension, which communicate over an end-to-end encrypted communication channel. All secrets are stored on the smartphone, and the browser extension is required to send a request to the smartphone if it needs to authenticate. The user authorises these requests by authenticating to the phone. This project aims to bring this solution to the market by developing a strategy that aims to explain the cryptographic trust mechanisms to non-technical users. Additionally, the current prototype should be developed into a mature and stable version with an intuitive interface. Lastly, a technical feasibility assessment will be conducted to discover if it is possible to decentralize the server component to be able to open source the core of the solution.

77	Deep Learning Deep-Learning Smart-Enhance Mobile Application that Makes Video/Image Enhanced by Processing Data in the Neural Processing Unit While Fully Preserving User Privacy Twitter: https://twitter.com/sensifai	Sensifai, **Belgium** Project Lead: Dr. Mohammad Hasan Bahari		image manipulation, personal data, privacy	There are different image enhancement app (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, scandalized 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. SensifAI have developed specific deep learning architectures for the new NPU chipsets of most major smartphone manufacturers. With this technology, the project can enhance users' images and videos locally on their mobile phone without any connection to the internet. With this project, Sensifai delivers on-device, smart-enhance app that can help millions of people enhance their video/image archives while guaranteeing control over their personal data. The project will also add automatic and realtime face and vehicle license plate detection/blurring system in future versions of the app such that users can avoid unwanted violation of other peoples privacy in public area while live broadcasting or sharing images/videos in internet.