The Alan Turing Institute

Trustworthy Digital Identity Conference

Progressing the conversation

January 2023

Contents

A Letter from the Conference Chairs

For its inaugural Trustworthy Digital Identity conference last year, The Alan Turing Institute brought together different perspectives from around the world to offer a snapshot of emerging risks and opportunities within what is often characterised as a polarised digital identity landscape. The day served to catalyse an important conversation wherein all can move forward rooted in being informed by the impact these systems are having on lives, communities and the relationships people develop with the organisations that they interact with every day.

In this second year, the Institute put a particular focus on the growing body of experience with government digital identity implementations. Such systems are being regarded as examples of modern practice and as such encourage widening adoption as they increasingly become a gateway to basic and social rights. They have sparked campaigns against their imposition and inspired initiative to reach those otherwise marginalised. Our conference reflected both perspectives while also delving into varied novel techniques for advancing the trustworthiness of systems and data management. We could see the conversation progressing to tackle the often-intangible risks highlighted in our first year, to enhance accountability, and to address prejudice or bias that can be embedded at the scale of which systems process data.

The conference opened with the United Kingdom's Information Commissioner's Office drawing much needed attention to defining practical interpretation guidance for largely principle-based data privacy legislation. Overall, the 14 sessions illustrate how digital identity is very much a social development with countries ushering in sweeping changes for the delivery of public and private sector services, and one call for the now widely-accepted Data Impact Assessment to be extended to include a Rights Impact Assessment.

Digital Identity has an amazing power to transform the lives of people. We are already seeing many examples of this around the world. Unfortunately, we are also seeing that it can be used to create harm. The team behind the Institute's Trustworthy Digital Infrastructure for Identity Systems research project chose to host this conference on September 16, a day increasingly celebrated as International Identity Day, in recognition of the UN sustainable development goal 16.9 to have identity for all by the age of 5. Digital identity systems are becoming fundamental to this goal, particularly within countries and regions where there are many of the estimated 1 billion people who lack any form of official identity document.

We are privileged to have welcomed about 100 delegates actively working with or researching relevant topics, bringing their perspective from North and South America, Asia, Europe and the United Kingdom. This conference makes a significant contribution to the work we are doing at the Institute to elevate and prioritise the knowledge needed to help people. We thank our project funders, the Bill & Melinda Gates Foundation for making it possible.

Professor Carsten Maple, Professor Jon Crowcroft, Dr Mark Hooper, Dr Lydia France

From Words to Actions

Gathering input in advance of a consultation on biometric systems, the United Kingdom's data and information protection regulator led the room through implementation considerations and navigation tips for varied open questions.

Current development in data protection legislation around the world tends to be based on now widely recognised data protection principles, laying out much needed flexibility to accommodate the context or use of the protected data. It also introduces challenges for system implementation with the body of experience and practical guidance this could underpin lagging the legislation. Our keynote address, an intentionally interactive session led by the United Kingdom Information Commissioner Office's (ICO) Clara Clark Nevola, worked to both acknowledge and address this challenge.

"What it means to be concise is not defined in the legal texts. There are no metrics set out for how readable something is," said Nevola, principal policy advisor with ICO's technology team.

"Principles in the legislation set out the spirit in which things should be done, and the goal you need to work toward," she explained while pointing out that this inherently means they need to be incorporated at the start of any project, to define intent and an effort to understand the impact on people and society. "Principles must be at the heart of what you are doing."

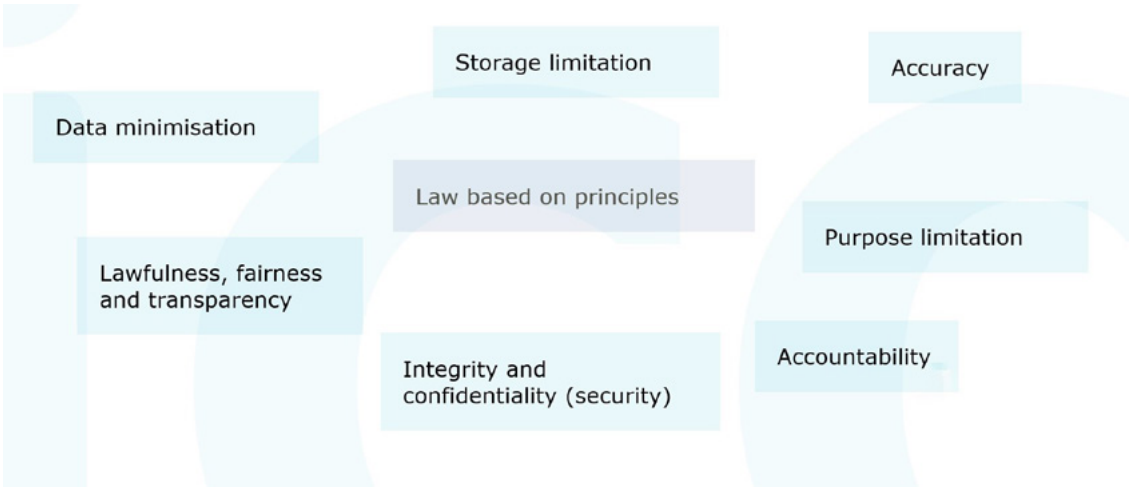


Fig. 1 Data protection legislation principles, as presented by Clara Clark Nevola during the Trustworthy Digital Identity conference.

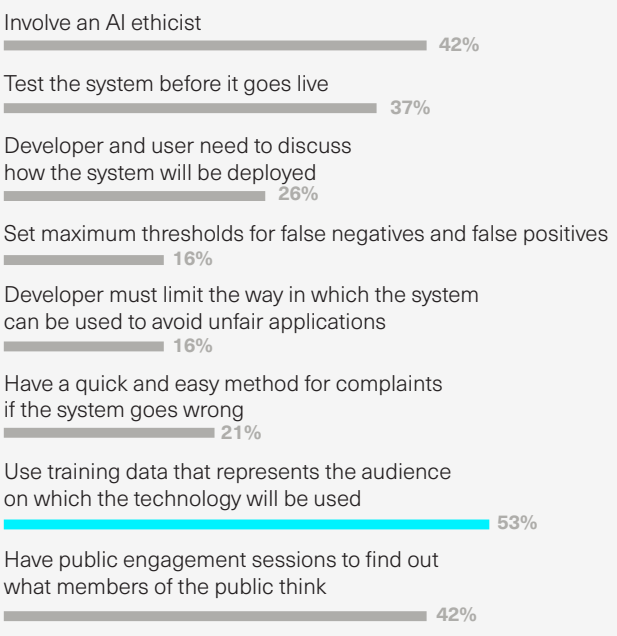
Outlining that the UK Data Protection legislation is largely principle-based, Nevola warned that following the prescriptive rules within the legislation is therefore not enough, later illustrating this point with the example of generic privacy policy statements.

“A general long privacy notice is not lawful. It doesn’t tell you how it (the system) works,” she said. “There is no silver bullet for every situation.”

“The principle of transparency requires clear, concise, easy language to explain what the tech is being used for and who is interacting with it. If you are, for example, using biometrics in a crowded area, do you need a big clear notice posted that captures attention and provides a route to knowing more, a QR code or flyer? What are the visual cues that tell you whether they know a device is recording biometric data? Do they understand it?”

Noting such questions speak to intentionality in design, Nevola declared that: “Transparency is the core of trustworthy systems. Trustworthy tech doesn’t happen by accident. We ask ourselves whether they are transparent, fair, secure because we care about these things.”

Audience response to Nevola’s interactive presentation. The answers outline ideas for the development of fair biometric technologies.



Nevola led the room through varied open questions inviting delegates' input in advance of intended guidance and consultation on biometric systems for release in 2023. Scenarios explored what fairness means in terms of purpose, methods of collection, impact, accuracy, and the steps taken to avoid discrimination or assure reparation when systems don’t work as anticipated.

“Consider a recruitment context, where biometric systems are used to assess emotions in the coffee lounge before an interview takes place. Is that purpose fair? Have you told people that the coffee break is part of the recruitment decision? How does a negative result impact people? Is the system sufficiently statistically accurate to be a basis for the effect it has?”

Noting that data accuracy includes the quality of biometric samples, Nevola pointed out that systems regularly returning high error rates or requiring multiple attempts to work are not accurate enough.

Describing the principle of data minimisation as “extremely context dependent” to reflect the stated purpose, she suggested the use of synthetic data where possible and pointed to the need to plan what happens to the data once the goal for collecting it is achieved: “If it is to be used for further purpose, is that further purpose fair and transparent?”

Suggestions from the delegates included the setting of metrics for measuring impact or trust in usage, forced disclosure of what the technology does, and the development of an organisational approach to maintaining the principles.
When asked for their top three techniques for developing fair biometric technologies, delegates overwhelmingly pointed to a need for representative training data as the top answer with the need for public consultation and the involvement of an AI ethicist, equally ranked as second.

Further guidance, as well more information about the upcoming consultation can be found on the ICO website.

The Rights Impact Assessment

Two very different national case studies, one from Brazil and another from South Korea, highlight how digital identity programmes fundamentally change how society is supported, elevating a need for more scrutiny on the path to benefit. They also shared common concerns as new concepts of "normalisation" rise in a post-COVID world.

Sessions focused on Brazil and South Korea emphasised the need to look past the advertised benefits that are significantly increasing the pace of digital identity systems deployment. Marina Meira, Head of Projects for Data Privacy Brazil Research Association talked about why her country's experience presents a case study for a fundamental rights impact assessment, while SaeByoul Yun, a PhD student at the University of Edinburgh questioned the blind acceptance of initiatives in South Korea's post-COVID society. While the economic settings and approaches to identity differ, both spoke to the growing risk of marginalisation.

Brazil's experience as a Global South country, one of the biggest and most populated ones in the world, is in the midst of modernising its state-issued foundational identity system, presenting a unique opportunity for understanding and mitigating risks to fundamental rights, proposed Meira.

"OECD (Organisation for Economic Co-operation and Development) measures Brazil as one of the top ten most digitised countries in the world.... That is not a bad thing definitely, but from our perspective, the problem is that it's being done without considering all residents", explained Meira. Pointing to the growing global body of data on digital identity initiatives in Global South countries, she expressed concern that such programmes are "advertised as a path to guarantee more inclusion and access to rights to all people...," yet often have the opposite effect, particularly for the most vulnerable.

Meira went on to outline her Association's project and policy paper, **Accountability and Digital IDs**, which calls for the now globally used Data Privacy Impact Assessment (DPIA) to be adapted as a powerful tool for also assessing fundamental rights violations.

"How we use data for public services is actually the trigger for any risks, both to individuals, and the data processing activities involved with digital identity systems. They are the entry point for the risk analysis to fundamental rights."

Meira talked through Brazil's Federal Government effort to digitise the delivery of 70% of its public services on its central Gov.br platform by the end of this year. She had been invited back to the Trustworthy Digital Identity conference for a second time after she and her colleagues shared insights on how quickly Brazil was progressing with its National Civil Identification programme (ICN). Bringing together functional and state-run public services databases, ICN had registered half the country's population and recruited over 500,000 citizens for a proof of life pilot to receive old age benefits.

This year Meira reported the system had become more embedded in Brazil as the pressures of the COVID pandemic encouraged what she called the "platformisation of public services." She raised particular concern with the growing use by Brazil's 27 States to authenticate citizens' claims for services before its resilience and coverage were fully developed.

"ICN is not fully implemented ... but it is very relevant in the national scenario at the moment because its database is now being used by the States to authenticate citizens using the Gov.br site."

"From the moment you establish that only people registered on the ICN database will be able to access the Gov.br platform, you immediately exclude people who don't have an ID from that platform, ... and of course, the tendency is that as the Government digitises its public services, it slowly abandons other channels."

Mapping the exclusion

Exclusion concerns being mapped by the state activity include people whose existing ID documents may not be adequate, such as transgender people facing slow processes with document recertification; children who do not get an ID document before 16 years of age; elderly people who are known in Brazil to have difficulties accessing the Internet, and people with disabilities who might struggle against biometric identification. Meira also noted that 19 % of Brazil's population did not have access to the Internet with this element of the population both unequally distributed throughout the country and overrepresented by black and poor people.

Data Privacy Brazil's proposal extends the DPIA with a special provision for a Rights Impact Assessment according to three conditions: That it represents a true judgment of how potentially excluded groups are affected; that it engages stakeholders inside and outside the organisation responsible for the data processing activities with the results made public as an opportunity for stakeholders to address their concerns; and that it be conducted before the implementation of a digital identity system, or any process related to it.

Prompting broader societal discourse

In January this year South Korea introduced a pilot for mobile phone driving licenses in two regions, and within six months opened the door for them to be used for wider purposes across the country. Holders can now verify their identity in community centres and banks and prove age and eligibility for purchases in convenience stores: Many private companies are considering linking the driving licenses to evolving payment systems. As she presented these developments, SaeByoul Yun raised alarm over the lack of evidence that the ethical concerns of such a wholesale change to how society operates has been thought through.

Yun shared findings from her efforts to research publications and media discussion covering both the mobile driver's licenses and another digital identity trial for government employees. She found that the public and government-led discourse is heavily focused on promoting benefits, such as convenience and cost savings, or the security technologies involved. "I believe that this period of trial is significantly important to figure out emerging ethical issues or problems... I believe we need a multi-faceted perspective to approach this issue," she said noting a dearth of evidence for such debate in Korean society. She noted

that the official government website, for example, offers little advice on what to do when a mobile phone with digital identity is lost or stolen or on who may be accountable for the impact should the owner fail to realise it was lost. Areas she proposes for more research would cover technical, legal, and ethical challenges, alongside the development of social consensus and education.

Yun observed that existing studies on digital identity in South Korea tend to focus on the technologies rather than their application, covering topics such as blockchain or QR codes. The few studies on ethics issues, such as privacy and protecting personal information, were over ten years old.

She also pointed to the impact Covid 19 has had on societal norms in South Korea, while suggesting that Covid passes, eventually issued in 140 countries, have set the scene for accelerating digital identity initiatives around the world. "Between 2002 and 2020 many governments introduced digital identity systems, but their acceptance had been relatively low for several reasons, including the need to address infrastructure and privacy concerns."

"As we know through Covid 19, many things have changed... it has become normalised for the public to show their status digitally with the introduction of vaccine passes. Many of the countries introducing these passes have integrated them with various certificates and insert them onto a mobile," she said.

"South Korea was one of the countries that accepted strong surveillance technology during COVID, but there were also lots of issues, for people who didn't want to be vaccinated, or could not be vaccinated. They just didn't get vaccine passes, so they didn't get into the cafes, and restaurants and were excluded from many social activities. There haven't been any solutions for them by the Government ...it's discrimination. There will be definitely some people who don't want to use or cannot use the Digital ID."

Despite identifying interest in security technologies, Yun suggested a need for a more comprehensive understanding of how risks are changing as private companies seek to use the digital driving licenses, pointing to their poor record against hacking attacks, and the amount of info contained in a mobile driving license, including personal choices around organ donation.

Digital Markets Driving a User-Centric Future

One survey indicates companies and organisations would welcome an opportunity to ditch proprietary onboarding for identity management.

Other developments, including a submission to the International Organisation for Standardisation (ISO) and the emergence of digital data markets, also contribute to influences driving a more user-centric future.

According to Sopra Steria's Tom Staley, commercial organisations are "stuck in the world of create" when it comes to serving customer demands. This is despite the vast majority, 85% of participants recently surveyed by the IT service management company, acknowledging that user-centric ecosystems are the future of digital services.

The survey of technology decision makers, 75% of which come from companies and organisations of over 3,000 employees, explored evolving developments with digital identity management within commercial and government organisations. Most respondents currently having to collect personal information or proof of identity with every customer account would welcome the opportunity to ditch proprietary onboarding, alongside the associated risks and administrative burden.

Findings reveal that the problem statement currently driving identity management across government and enterprise tends to be focused on legacy processes, including concerns around security and data privacy issues. "They did not report an issue with the backing of senior management or lack of funding for new systems, however fundamental concerns with the challenge of moving away from existing ways of doing things, means legacy services are holding them back," explained Digital Identity Consulting Lead Tom Staley, while describing new pressures from post-Covid expectation for "digital ways of proving identity without physically having to attend somewhere and show it.

"The ability to collect, reuse and manage identity data and attributes in a way which can be securely shared, and offer user empowerment with the flexibility to share different personas, preferences, or tastes are recognised as the future of digital services," he said while acknowledging they require levels of collaboration and trust in data that is currently difficult to achieve across competitive industry landscapes.

Staley forecasted that recognised benefits around customer or citizen experiences and efficiencies will prompt markets to move from single organisation focused use cases often relying on biometrics to multi-organisation use cases that address common industry problem statements in the medium term, and eventually "true cross domain, boundaryless and borderless digital identity in the long term."

To reach this future Staley characterised four stages on the roadmap to digital identity adoption and noted organisations are at various points on this journey: Looking In, Looking Up, Looking Out, Looking Forwards. These begin where most companies currently exist on this journey with the use of existing processes and service delivery models and move through the use of an identity across an organisation, cooperation with external partners around a specific use case, and eventually active participation in coordinated market initiatives to develop connected ecosystems. He also recommended that companies begin engaging with complementary organisations to establish collective approaches to current market problem statements.

Referencing the Open Identity Exchange estimate of six million UK adults who are identity challenged in a digital society, he advocated that organisations adopt end-to-end, user-centred design in service delivery and a focus on outcomes across their business.

"We reside in a digitally advanced, developed economy, where 10% of the population doesn't have access to foundational documents... how do we consider those from an ethical perspective that actually doesn't have access to the foundational documents that our existing processes depend on. What's the benefit we're going to deliver to citizens, to governments, to enterprise...?" he challenged.

Decentralised user-centric data marketplaces

The emergence of international, borderless decentralised data marketplaces offers a snapshot into how digital economies may be evolving. City University of London-PhD Student Akanksha Dixit talked through developing opportunities for digital trading as it supports more and more intangible goods, from digital art, music, and photography, to, increasingly, the data generated by the sensors in industrialised IoT and connected home systems.

"We are seeing the rapid increase in the industrialisation of data production. This data sits in silos, in different organisations, in different factories and home environments ... including data from agriculture, weather patterns, traffic patterns generated by both public and parties.

"Decentralised data marketplaces will allow such organisations to monetise this data," she predicted, anticipating the opportunity for such data to be sold in bulk or by subscription as it is continuously generated.

With current digital trading dominated by platforms where creators offer no visibility or control over how products are marketed and sold, Dixit reviewed elements of her PhD paper for underpinning fairer trade. Her proposals outlined a distributed architecture for reliably verifying buyers and sellers, and establishing transparency in the supporting processes.

In describing the current dynamic, Dixit highlighted that: "Once a product is listed, rights and control are transferred to central entities (running the platforms). Buyers do not decide the terms and conditions, or even the profit of the trade... there is no clarity on how the recommendation system is designed for each product."

Dixit's proposed architecture exploits a blockchain ledger network that authenticates buyers and sellers and automates the execution of smart contracts according to discrete arrangements made between them. Such marketplaces would also host the data and process transactions through decentralised networks.

"There's a lot of work going on in the Internet community now moving back to peer-to-peer-based models," she explained, adding markets will advance with confidence over time as they document user accountability and mature with the development of standards to underpin digital asset transfer exchanges. The use of privacy enhancing technologies could also be applied to personal data generated by wearable tech, such as smart watches. "The approach is designed to help with traceability, enabling user authentication and authorisation, the tracking of tampering ... and helps with better negotiation capabilities."

A new standard for transparency

Zero Public Network's Mark Lizar reinforced our keynote speaker's call for transparency to be the core of trustworthy systems as he outlined work on Notice Records of consent submitted to the International Organisation for Standardisation (ISO). He also established their importance, referencing research into the Android platform determining that 73.1% of the applications disclosed data with third parties without giving notice.

"Less than ten percent had any type of notice of consent, and of those only 3.5% obeyed the consent. A (consent) withdrawal signal was sent, and they still gave access... This is a massive security breach because now we're seeing big data being used to attack systems and little control for anybody to actually protect themselves in the context of using a service online."

"Zero public network means your data is never exposed without a (data) controller being identified," Lizar explained as he introduced the proposed standard for an Operational Transparency Specification for Notice Records and Receipts.

"The idea is to be able to give a person a record of when they consented so they can track and see how their data is being processed and, most importantly, how has my privacy changed?"

Contrary to common understanding, control over data and associated consent for its use is in practice governed by contract law, not privacy law whenever individuals tick a box agreeing to terms of service, Lizar highlighted.

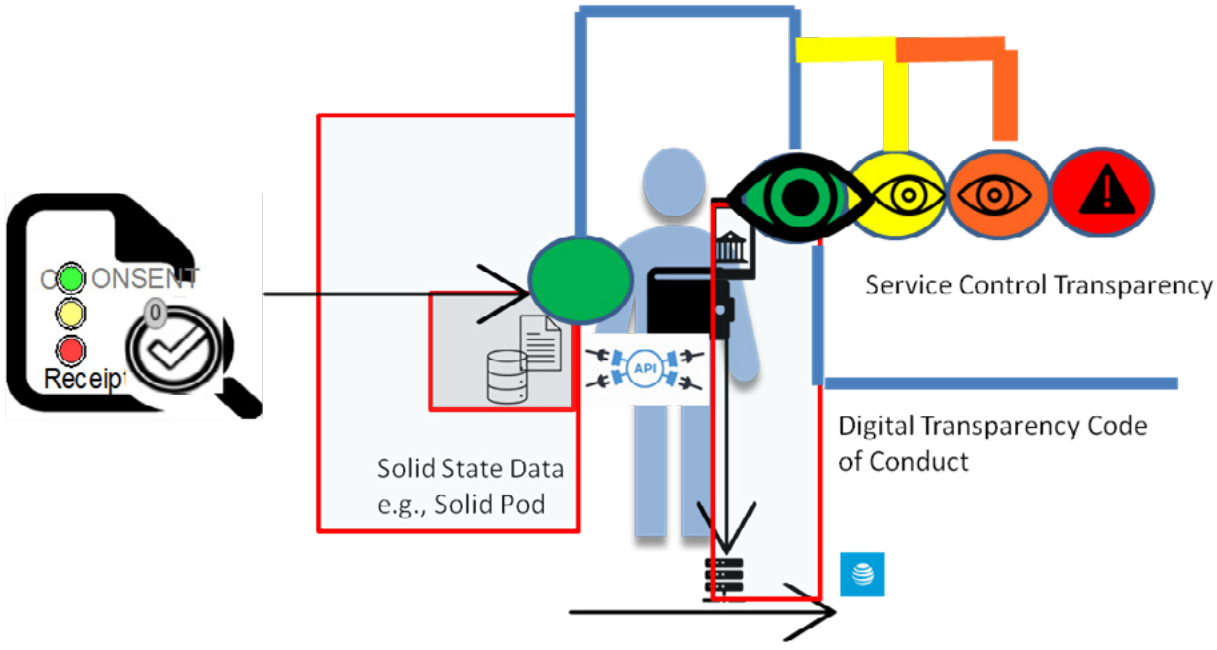


Fig 2. Privacy as Expected: the human consent gateway with notice records (micro-credentials) and consent receipt tokens, as presented by Mark Lizar during the Trustworthy Digital Identity conference.

"That's the big hack, the dark pattern that causes the most problems that's enabled contract-based governance to dominate services online," he said.

Lizar also noted a lack of consistent understanding of the concept of transparency across countries and digital identity and privacy frameworks and explained that data moving between organisations is disclosed not shared, stressing that each disclosure point requires a new privacy or data control impact assessment. Notice Records give people a standardised receipt when this occurs and the agency to allow, withdraw consent or restrict processing as data is disclosed.

Written as a public infrastructure, non-national standard for international and internet scalability, a two-factor notice, (which the writers we like to see coinciding with two-factor authentication) prompts choice and then generates a signed consent receipt token specific to a purpose. A red-yellow-green notification system indicates a change in privacy state with the involvement of a new data controller and purpose, giving the user agency to respond and accept or update their choice. The user gets a proof of notice record, replacing the tick box to agree to terms of service.

Addressing the potential for objections based on technical barriers, Lizar suggested the technical capability to implement Notice Receipts already exists pointing to techniques deployed within organisations' digital assurance systems for accessing databases and files and sophisticated systems underpinning personalised advertising.

Emerging Techniques for Security & Governance

The limitations of adapting general systems security to identity systems is inspiring innovation for advancing ground-up security techniques. Sessions featured this year covered a new neural network machine learning model for cyber risk estimation; automated red teaming; homomorphic encryption for cloud-enabled scalability; and decentralised public key infrastructure.

Privacy-preserving identity verification using third-party cloud services

Working with the scalable and cost-effective computing power offered by cloud service providers is an increasing imperative for national identity systems as they evolve to support significant populations and an increasing scope of services. However, moving citizens' sensitive and highly targeted identity and demographic information into the cloud presents particular challenges for assuring privacy and security, including concerns around political interference and regional compliance requirements when the cloud provider is based in another country.

Dr Srinivas Vivek, International Institute of Information Technology Bangalore showcased the Institute's Modular Open Source Identity Platform (MOSIP) project which allows for the privacy-preserving use of cloud services by ensuring that raw, unencrypted citizen data never has to leave government servers. Modelled on India's Aadhar digital identity service, which has transformed the delivery of public goods and services in the country, MOSIP is supporting countries across Asia and Africa, and has enrolled about seventy million people.

Using homomorphic encryption, which allows data to be analysed and processed without being decrypted, the project uses Microsoft SEAL libraries and incorporates Boolean calculations to deploy encryption efficient enough to support authentication and rights of access queries.

"Contrary to the popular belief that these technologies are slow, we show that biometric and demographic queries can be performed in about 0.3 seconds ... and also the amount of space needed for the interpreted data is also quite feasible, about one megabyte per user," said Vivek.

MOSIP gets around the bottlenecks that traditionally

slow the processing of encrypted data, with an encoding scheme for packaging and evaluating select packets of data (with low multiplicative circuits). The load on centralised government servers is minimised as the bulk of query computation occurs in encrypted form on the cloud servers. The data is encoded to allow for the recognition of given characteristics, such as an age limit, to authenticate a user's right of access to a given service. User data is stored as two sets of ciphertexts: Demographic data such as name, age, etc; and Biometric fingerprints to support three types of queries:

1. Direct demographic matching: directly comparing name, gender, address, etc.
2. Age comparisons: Comparing age against thresholds. E.g. is the user younger than 18 or older than 65 years?
3. Biometric comparisons: Comparing and verifying matches on encrypted biometric template

Preliminaries in Automated Red Teaming in Hardening Digital Identity Management Systems

Research Fellow Dr Anh Tuan Le, University of Warwick, presented the scope of his project to develop automated red teaming (ART), a technique which is gaining traction in general systems security management, for identity management environments.

The project is working to integrate new knowledge into the MITRE Adversarial Tactics, Techniques and Common Knowledge (ATT&CK) framework for general security, bringing together tools such as Identity Threat Assessment and Prediction (ITAP) and automated language processing to translate security knowledge from reports, and build vocabularies. The scope of work includes establishing a community to develop best practice and knowledge peering, alongside the development of AI, applications and metrics to enhance the capabilities of the MITRE framework's focus on identity security.

Explaining that ART relies on developing tools and techniques for understanding the relationships between assets, their vulnerabilities, and attackers' goals to create testing scenarios of real attacks, Tuan Le described varied challenges that have hampered the development of effective approaches in identity management. These ranged from the immaturity of knowledge databases relevant to identity management systems, the role of these systems to open many doors to services, creating a "huge and complex attack surface" and the complexity of the systems themselves, supporting AI applications, remote users, and increasingly decentralised architectures. "It is difficult to replicate operating environments which are influenced by many dynamic factors such as transaction rate, latency, network conditions... as well as test compliance and restrictions on the sensitive personal data that is subject to data protection laws such as GDPR," said Tuan Le.

Tackling these challenges to develop ART for IDM systems, researchers aim to:

- Enhance the training and understanding of security insights through realistic emulations
- Enhance insights into risk exposures including costs, compliance, reputation and other concerns
- Help decision makers understand how their assumptions and biases can impact the effectiveness of their decisions
- Improve risk assessment accuracy, and readiness to deal with constant changes in attack on identity management systems

Decentralised Public Key Infrastructure

Acknowledging limitations with blockchain ledgers, Dr Tim Hobson, presented a proposed solution from The Alan Turing Institute's Research Engineering Group for decentralising public encryption key infrastructure for identity attributes. The open-source software solution anticipated to be available by the end of 2022 embeds existing trust relationships between real-world institutions to eliminate the prevalence of relying on a generic certificate authority.

The Group developed an extension to the World Economic Forum's WC3 standard for verifiable credentials and deployed the InterPlanetary file system (IPFS) protocol for storing the public key information in a distributed file system. Chains of trust are created by linking decentralised identifiers that can be independently verifiable using a blockchain ledger's timestamping of data entry.

"Unfortunately, the word blockchain has become a bit of an industry buzzword, and it's often hyped beyond reasonable expectations. We really wanted to recognise some home truths about what you can expect of this kind of decentralised technology," explained Hobson, senior research software engineer, Turing. "I think it's fair to say that the proof of work consensus mechanism enables us to produce verifiable timestamps. I would argue that nothing else is independently verifiable."

In the proposal, verifier registries are created with a root of trust transaction whereby a collection of trusted organisations that recognise each other and share a common interest in linking identity attributes register their public keys as a well-publicised event. Once the root transaction has been observed by all participants, they publish downstream transactions linking together identifiers to digitally create chains of trust.

"You could have this at a global level with organisations such as the World Bank, European Union, and African Union, or you could have this on a much smaller scale," he said, noting the possibility for interoperability between the foundational or functional systems that currently exist, including between countries. "They (the organisations) essentially sign each other's credentials, and then a verifier can trace the chain of trust all the way back to the root which is timestamped, assuring confidence in the public key information."

Hobson illustrated the work with an example of an anticipated use case: "You could have a central government entity in the root, the Department for Education as a subordinate, and each university would then have a certificate. A verifier (of the certificate) can verify the links in the chain of trust, each of these institutions is recognisable, and appropriate in that chain of trust."

He went on to describe how permissions can be delegated in a granular fashion, and nodes moved around to increase the scope of a

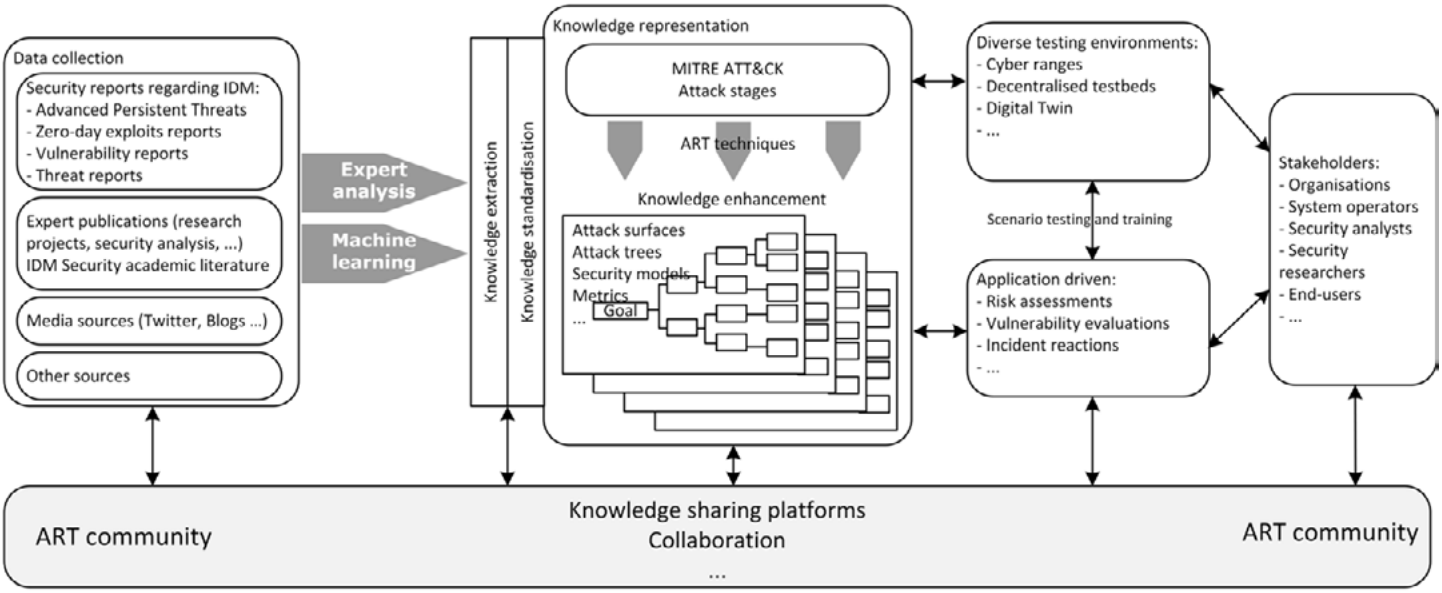


Fig 3. Strategies for applying automated red teaming in identity management environments, as presented by Dr Anh Tuan Le during the Trustworthy Digital Identity conference.

system by transferring credentials that have already been issued from a smaller system.

"This attestation is very, very transparent. These are existing trust relationships that we all would accept offline," he said, concluding that, "any community can just create their own root of trust. It's an open protocol."

A novel federated learning method to model cybersecurity risk estimation for digital identity management systems

Po-Chu Chen, data science research assistant, University of Warwick presented his work to assess the potential of federated machine learning, a technique introduced by Google in 2017, for privacy-preserving assessment of current and emerging risk estimation of digital identity systems.

Analysing characteristics or values related to data, federated learning avoids the need to reveal the raw data to perform analysis. Initially developed to speed up machine learning performance, the team is exploring opportunities for also improving accuracy to levels reflective of more widely used centralised machine learning. Further, Chen highlighted opportunities to assess decentralised identity management systems and move away from the shortcomings of varied current systems, including the prevalent proprietary systems that require the creation of multiple user credentials and centralised single-sign-on models, which present significant risks for the user in the case of failure.

Working with 12,000 items of simulated identity data, researchers modelled a hierarchical structure for device-level risks, identifying specific risk criteria and sub-criteria, that include parameters such as user behaviour and efficacy of control, alongside technical vulnerabilities. Metrics were developed for each to create a neural network model specific to identity management systems and then tested using three federated learning algorithms, SSGD: FedAvg; Semi-ASGD: SAFA; ASGD: FedAsync.

"We were able to dramatically shorten the training time (compared to central machine learning) using federated models, which allow us to assess huge systems and we could address issues for assessing a privacy sensitive environment," he said, explaining that federated machine learning as it performs the training on client systems using local data, accommodates challenges particular to the highly heterogeneous cross-organisational environments typical of identity systems. "It's difficult to track security requirements from component-driven risk analysis to system-level business impact."

Researchers concluded that while all three methods can provide high-accuracy results, the Asynchronous method provides outstanding training performance as it was particularly suitable for the highly heterogeneous environment. Chen also recommended complementary research to test the methodology on decentralised digital identity systems and work to advance privacy-preserving access to user data to develop the model further.

When the Room Hums...

"When the room hums, it usually means everybody is in favour," noted Professor Jon Crowcroft in the closing summary with Professor Carsten Maple as the conference co-chairs highlighted a coalescence around particular themes of the day.

A key thread across the sessions pointed to a developing deference for decentralisation, alongside techniques to support the idea of not having to take the data out of people's hands. This is a theme that covered full identity systems architectures to component processes such as authentication, participation in digital economy markets and machine learning models for risk assessment.

The co-chairs reflected that the decentralised agenda is not a new thing for the Internet: It dates back to the IP routing protocols that established it in the 1980s. While current business models monetising data have in effect recentralised things in many ways our conference demonstrated that this state of affairs has also inspired work to decentralise again in the pursuit of fairer trade, user-agency and the desire for a more user-centric services environment. Many organisations, commercial and public, that have tried to own identity systems are beginning to appreciate the costly administrative and systems bottlenecks involved and are ready to make their contribution to the decentralisation story.

There is, however, no reason or need to anticipate one approach as governments and organisations continue to develop centralised services to suit their objectives. Whatever the approach, another core theme from the day's sessions illustrated that the development of digital identity is unavoidably political - the policy, legal, regulatory and technical must be interlinked with each other. We all need to learn the languages of these elements and appreciate the breadth of expertise to be embedded in the journey toward trustworthy systems, from the AI ethicist and the security and systems engineer to the legal and data protection officers, so we can move forward together.

The playlist containing conference recordings is available on The Alan Turing Institute YouTube channel.

Join the conversation

As governments around the world adapt to an increasingly digital and global society, more than 80% now rely on some form of digital national identity. Whilst this development can offer significant benefits, digital identity systems can also pose considerable risks and exacerbate inequalities. The Alan Turing Institute's Trustworthy Digital Identity Interest Group brings together a vibrant, global community of over 100 practitioners and researchers who meet regularly to host a vital discussion and investigate the evolving technical and social risks and contribute towards the development of more trustworthy systems.

Learn more and apply to join.

The Poster Tour

Four academic posters featured on the conference agenda. These contributed insights relevant to the ethical facet of trustworthy digital identity, delving into impact stories on societal accessibility and fundamental rights. Two focus on exclusion, covering opportunistic societal bias in Ghana and why campaign organisation Access Now suggests biometrics should not simply be treated as personal data. The other two posters offer perspectives on empowerment, including a programme of social support for HIV-positive young girls in South Africa, and, a personal capability model supporting pregnant women in Nigeria.

Is the Capabilities Approach an operationalizable lense

Henk Marsman

Outcomes

The CA can be operationalized as a lens through which to view the impact of digital identity (DI) systems on human lives.

The emphasis on the individual and opportunities in a context and human development in the CA addresses the impact on human lives.

Ndaga Muntu as a Case of DI

2021 report by CHRGJ documents cases of exclusion and rights infringement of individuals due to failure of having or being able to use a National Identity Card (DI) in Uganda.

Critical services are walled behind DI.

Assess with Capabilities

To correct wrongs a legal approach can be applied. The author proposes an approach that is able to assess the broader impact on human lives and their development (improvement): the Capability Approach (CA) , by Amartya Sen.

Is this approach feasible?

The commentary investigates whether the Capabilities Approach is a feasible and implementable approach.

Once this is established the comparative analysis to other assessment approaches, such as Affordances, needs to be conducted.

CA and Technology

The real impact on human lives of technology examined with the CA illustrated by the case of mobile phones for pregnant women in Nigeria. CA describes new capabilities in a participatory approach, and highlights the influence of personal, social and environmental factors on conversion of these capabilities.

Contact

Henk Marsman
Thinking Through Digital Identity
ThroughIdentity@proton.me
+31 6 5133 7490
https://henkmarsman.wordpress.com/
https://www.linkedin.com/in/henkmarsman/

The rapid growth of biometric technology for identification

Marianne Díaz Hernández

Biometrics are increasingly used in ID systems

They are promoted as a “catch-all” solution for legal identification, which can tackle complex issues such as distribution of benefits, identity fraud, and more.

Soft and hard biometrics in identification

Hard biometrics: collectability, universality, uniqueness, permanence

Soft biometrics: multimodal systems

Current legal approaches to biometric data are insufficient

The collection of biometric data can raise concerns and discomforts, can be seen as invasive, uncomfortable, humiliating or frightening; can cause additional exclusion, and can further issues of truth towards authorities.

Collecting data about the body isn’t about data protection

Claiming that the use of data extracted from the body only affects the information and not the body itself denies the inextricable relationship between those pieces of information and the dignity of the body to which they refer.

The issue of consent

The automated nature of most biometric data collection practices by itself excludes the possibility of prior consent. Furthermore, the absence of alternative denies consent as a possibility altogether.

Contact

Marianne Díaz Hernández
#WhyID Campaigner
Access Now
marianne@accessnow.org

Biometric IDs and Exclusions among the Fulani in Ghana

Isaac Owusu Nsiah

Outcome: Fulani relational encounters with ID systems

- Politicization of IDs: *Logics of state and political power and their impacts on the Fulanis ID inclusivity and exclusionary tendencies.*
- The Ghanaian state's non-recognition of the Fulani as an institutionalised identity or ethnic group
- Bureaucratic partiality and offensive process: Deliberate, unapologetic attitudes by bureaucrats and procedural barriers in ID acquisition.

Othering and Marginality of the Fulani in Ghana

Politics of citizenship(ambiguities of colonial and post-colonial constructions of who belongs and belong less)

State-Fulani relation(realities of expulsion)

Prejudice and stereotypes; social cognitive categorization of Fulani as foreigners

Background and Objective.

- About 500million marginalized groups in Africa are without IDs
- About 75% of state bureaucracies have institutionalized digital/biometric IDs in Africa
- Social and institutionalized exclusions persist among marginalized groups amidst digital IDs
- Existing literature on technical and regulatory factors
- This research analyzes exclusionary impact of digital IDs as complex historical, social and political phenomenon
- Explore subjective experiences of 2nd or 3rd generation Fulani in accessing Identification documents in Ghana

Methodology

Qualitative research methodology(Phenomenology)

-Study area: Agogo, a town in the southern part of Ghana(Ashanti region)

Participants: 2nd or 3rd generation non-pastoral Fulani and sedentary pastoral Fulani and descendants; Leadership of the Fulani in Ghana.

IDs: *Ghana card, passport and voter ID*

Methods: in-depth semi-structured/unstructured interviews, focus group, key informants interview.

Contact

Isaac Owusu Nsiah, PhD candidate, Institute of African Studies, University of Ghana(Legon),+233(0)547209777
isaacnsiah88@gmail.com

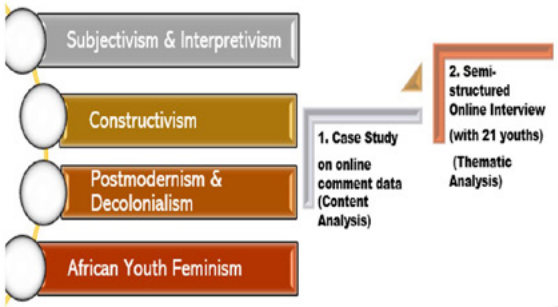
Identity Re-construction via Digital Interactions among South African Youths (16-28) living with HIV

SunHa Ahn
Supervisors: Prof. Jude Robinson & Prof. Bridgette Wessels

Finding

- 21 young participants (16-28) in South Africa commonly said that buying mobile data is very expensive (a substantial social barrier).
- Getting mental support and lived experiences like life lessons around HIV is the main reason for internet use. This is linked to whether to sustain their treatments and how to live with HIV.
- Social or relational capitals (trust issues) feed into virtual activities. Through relation expansion, HIV young women and girls create a comfort zone and supportive system online.

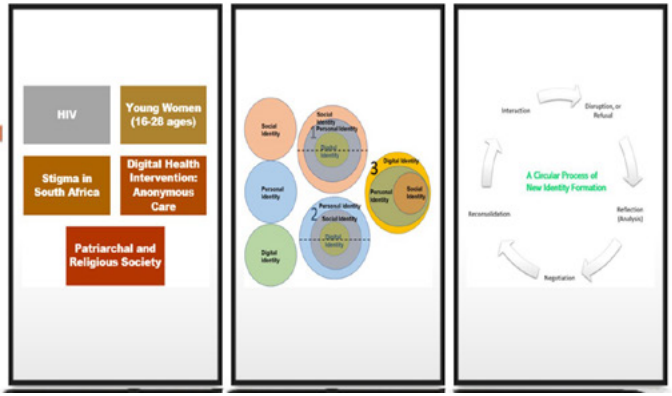
Methodology and Methods



Background & Concepts

- **Aim**: Through a dynamic online interactive process, the research expects the potential therapeutic role of anonymous digital activities, alleviating rampant social stigma among young SA women and girls. It is called social identity reconstruction online.
- Sociological and socio-anthropological approaches
- **Identities**: Personal, Social and Digital
- A circular process of the new identity formation:

Interaction-> Disruption/Denial-> Reflection-> Negotiation-> Reconsolidation-> Interaction (again)



Discussion

- Stigma around HIV, stemming from religious faiths and patriarchal aspects, is closely related to knowledge gap by generation.
- Socio-economic inequality is growing along with the digital divide (linked to job opportunities) or information reliability (spreading misinformation about HIV)
- Digital accessibility is a survival issue and a powerful way to prevent vicious cycles caused by knowledge gaps.
- In the context of the Covid-19 pandemic, using anonymity on SNS platforms, especially for socially stigmatised groups, helps mental support.

Contact

SunHa Ahn
University of Glasgow
Email: s.ahn.1@research.glas.ac.uk
Web:https://www.gla.ac.uk/pgrs/sunhaahn/
LinkedIn(mywayssunha);Twitter: @ssunha

Hosted by Trustworthy Digital Infrastructure for Identity Systems, a research project from the Alan Turing Institute.

Follow the progress **#trustworthyid**
www.turing.ac.uk/research/research-projects/trustworthy-digital-infrastructure-identity-systems

Twitter **@turinginst**
LinkedIn **school/the-alan-turing-institute/**
Sign up to the newsletter: **www.turing.ac.uk/contact-us/join-our-mailing-lists**