Freedom Not Fear session on privacy in e-governance: “How can the Erasmus generation enjoy the charms of electronic services without losing their privacy?”

organizer: Thomas Ruddy

announcement of session with readings,
https://pegasus.thomasruddy.org/programme

Cross-border lives during the course of your education leads to sensitive data travelling across borders several times. Look at Kaliya’s life stages: (Kaliya: https://identity-woman.net/)

as a teen: her school ID, transcripts, recognition of academic degrees

medical: EHIC + eSOS

worker: social security contributions, totalisation

financial: e-banking standards, HCBI, tax labilities

certificate of partnership (marriage)

old age, death, inheritance

There are cross-border eID projects to facilitate all of these processes. General Identity Management Law is the name of the legal field, a part of General Commercial Law

ID paradigms: (see e.g. https://identitywoman.net/topics/my-papers/internet-trust-models/)

centralised

federated (multiple authorities control the data, e.g. cross-university library cards, eduroam)

user-centric

self-sovereign (e.g. using blockchain)

World’s largest ID programme is in India, which is registering its >1,2bn citizens. The supreme court made a ruling setting constraints in favour of citizen privacy
The World Bank has a programme “ID for development”: (ID4D) http://www.worldbank.org/en/programs/id4d – eID is actually part of the UN’s sustainable development goals (SDG)

speaker: Frank Leyman, works for the Belgian ministry for Policy & Support (BOSA) “Digital Transformation Office”

Why e-services: make life of citizens and industry better. Basics: citizens (national register), companies (industry register), territory (cadastre).

Interesting different solutions in various countries:
Austria:pure virtual
Belgium: just a keycard to open (virtual) doors
Estonia: e-Residency
Malaysia multi-application card
Moldova: Mobile ID
UK: private sector: 8 private companies appointed to auth citizens

Challenge: make the various systems interoperable

The Belgian identity card is used as a “key” to open the door to web services from all ministries under http://www.belgium.be/ → https://mybelgium.be/ (no applications on the card itself). Companies do not receive separate IDs btw, representatives use their ID which is then linked to a role in a company, to use services on behalf of companies

eIDAS (electronic IDentification, Authentication and trust Services) is the underlying EU regulation (https://en.wikipedia.org/wiki/EIDAS) for cross-border electronic identification and trust services like web authentication, time-stamping, archiving and electronic signatures.

Example: French person needs to declare taxes in Belgium. Surfs to website of BE ministry of Finance, clicks on EU flag, then French flag, gets redirected to French auth server, picks a method and identifies to server in France which then sends result of the handshaking procedure back to Belgian server

Conclusions:

Increased efficiency has a (small) cost in privacy

Privacy Commission must guard the privacy (data) of our citizens

Education is required, people must be aware of what is happening

Opinion: eID ha made life much easier.

Q&A with Frank Leyman

Q: Principal / Agent problem: a manager might act in their own interest, not that of the company they represent.
A: eID is a knife that cuts both ways. There is a potential weak spot, i.e. a civil servant in a municipality has access to the register used by all citizens in that place, logs in with their eID in the morning, actions can be traced. The higher rank a person has, the stronger the penalties are.

Q: How about open-sourcing the technology?
A: We defend open standards and open source. Source code to eID has been put online and is open to amendmends and comments. Experience is exchanged between CIOs from member states, most do a lot in open source. Public tenders require open standards and ask for open source

Q: Could I make my own smartcard that speaks a defined protocol and use that in your system? Could we get to the self-sovereign system that we talked about earlier, create an identity that the government does not hold the private keys of?
A: “That would be dangerous …” Technicalities are published and free to consult, but we will of course not publish our private keys for creating the certificates that we accept. Two pilots were created named Stork and Stork 2.0 (the bird became the symbol for eID, the stork brings children and is a migrating bird). http://joinup.ec.europa.eu/

Q: Can people add their own information to their own records/accounts? Could it be possible perhaps to implement a happiness index in the future, were people supply the data?
A: As a Belgian citizen I can go to the national register and view the complete data they hold about me, including history, documents, status, relatives. I can also see when a civil servant entered my data and I can ask for an explanation why the data was entered. To respect civil servants’ privacy, I cannot see their names. (National security reasons can cause information to be unavailable.) Regarding the “file” behind the ID, tools are being developed for things like a unique e-mail address, and ask for communication to be sent to that address. Identification tools will be able to be stored in a profile. Progress on this is slower than e.g. in Portugal (e-mail project already live).
Recently in Tallinn countries have committed to allow citizens to interact digitally with public administrations", page 4 of this PDF, https://www.eu2017.ee/sites/default/files/2017-10/Tallinn_eGov_declaration.pdf

Q: How is security ensured? External audits? Admin access to the database?
A: The private sector runs the data centers, they report back to us (project managers in the government). Various restrictions for access have been put in place.
Q: What do you require from these companies?
A: Standard certification procedures.

Q: This is critical infrastructure. Why have you put this in the hands of private companies?
A: Budget, competence, time to market. Governments have previously tried to be experts for everything, we have learned that we can gain the latest expertise much faster by outsourcing it to the private sector. We only really need to be in charge of the project and set the right terms.

Q: Why hide access by police and secret services?
A: This rule was not our invention, it is more or less standard in several countries.

Q: Do third party exceptions need a warrant for access?
A: yes
Q: If I am under investigation later and there is a warrant, can present data be accessed?
A: There is a case when a famous singer died, civil servants accessed his personal data. This was found out and they were penalised.

Q: Is it part of the privacy commission's work to consider the ethics of hidden access by police or secret services?
A: Police and secret services comply to a different law. Only politics/parliament defines those laws.
Q: For me as a citizen it might be very valuable to know that services tried to access my data, I might want to ask the services why they wanted to access. If I am a criminal then government access might make me reconsider my actions.
A: Personally I agree, it might be interesting to hear this from Denmark.
(Q: It is possible in Estonia.)
A: Maybe Belgium is not top of the rank in openness, but I think we're doing okay and moving forward. The more you go south in Europe, the more closed the systems tend to get.

Thanks go to Sebastian for note-taking.