White paper on Data Driven Urban Infrastructures and Trust Frameworks ID^3

By Shenja van der Graaf and John Henry Clippinger

It's about using ICT to capture, spread and process information: to deliver urban services that are better and more integrated. It's about cutting waste, cutting unnecessary emissions and cutting the use of scarce resources. It's about tapping into the potential of our people: empowering them to organize their own communities, and improve their own environment. And, usually, we find SMART at the interface: it is where sectors converge that we can see huge innovation and huge environmental benefits. SMART sounds simple. But it is not. It is unlikely to happen by itself: not quickly, anyway. (Neelie Kroes, Vice-President of the European Commission responsible for the Digital Agenda, 10 July 2012)

Urban performance and urban competition rank high on the European Union (EU) agenda in its aim to achieve urban growth, thereby highlighting the term 'smart' to describe the next stage in city and regional urbanization processes. In this view, it can be seen to, particularly, capture a combination of hard infrastructure, information communication, social and environmental infrastructure rather than the role of ICT infrastructure per se. And, while the term is a seeming problematic one and the focal point of definition can vary from utilization of infrastructure, to the role of creative industries, and to collective intelligence (Holland 2008) so as to provide better and more efficient infrastructures and services, often for less cost, this is not discussed here.

A 'smart' example: European Platform of Intelligent Cities (EPIC, ICT PSP) is a scalable and flexible cloud based platform for the development and delivery of innovative city services. It uses innovative 'Future Internet' technologies such as 3D-geolocalisation for mobile devices, mobile sensors, and augmented reality to create truly smart, cost effective eGovernment web services such as relocation and urban planning applications. And, is accompanied by a practical guide to help cities deploy the EPIC platform to enable them to become smarter through the delivery of more effective and efficient services.

What is at stake are the data involved in these urban infrastructures that underpin government services and also transportation, energy, housing, education, retail, recreation, health and wellness, and so forth. More specifically, the delivery of government services could become vastly more efficient, less costly and more effective in serving the needs of cities and their citizens if it were possible to capture and share personal and group data, sensor data, aggregate and data-mine, analyze data to anticipate problems and provide more efficient and timely delivery of services.

There are, however, several barriers to overcome such as challenges that concern collecting the data (of e.g. cell phones, sensors), the use of different data bases to store the data, the processing, analysis, visualizing and sharing of them for different service needs at the government level, at the individual level, at the retail level, etc. Also, the volume, velocity and variety of dynamic data associated with data driven urban infrastructures is rapidly increasing, and which is referred to by the rather poorly chosen term, 'big data' (cf. boyd and Crawford 2011). It raises whole sets of new concerns such as about information quality, and transparency and openly use of the data so to reduce or refrain from severe implications for privacy and security.

Data have thus enormous political and economic power, and hence, abuses in their acquisition and use are of critical importance. Harms result from unprotected and unwanted disclosure and from a lack of sharing and use.[1] Yet, rather than one piece of regulation, several EU directives exist that deal with data protection issues.[2] And, moreover, how do Europeans themselves practice and perceive of issues that are concerned with personal identity data management?

Data protection, privacy and electronic identity in Europe

In a recent study, JRC (2012) examined behaviors, attitudes and regulatory preferences of Europeans with regard to data protection, privacy and electronic identity on the Internet in particular, and in their everyday life more generally. For this study 26,574 interviews with people, 15 years and older, derived from all member states, were conducted. The key finding is that "personal data disclosure is increasingly prevalent" in Europe, and that "most services provided […] rest on the assumption that these data and associated electronic identities are collected, used and disposed of according to existing legislation" (p. 15).

It was reported that about two thirds of the respondents use the Internet frequently. About one third uses social networking sites and about four out of ten said to make online purchases. Personal information such as biographical and medical gets

---

[1] Principles such as Personal Identifying Information (PII) and kinds of Fair Information Practices (FIP) are artifacts of an era of mainframe computing where the key harms were considered to be the unauthorized disclosure and use of personal data. But with social networking, networked enterprises and so forth, harms resulting from inappropriately sharing data can be as grave.

[2] Including, Directive 95/46/EC (protection of individuals with regard to the processing of personal data and on the free movement of such data); Directive 1999/93/EC (framework for electronic signatures, and the proposal for a revision of the eSignature Directive with a view to provide a legal framework for cross-border recognition and interoperability of secure eAuthentication systems [DAE Key Action 16]); Directive 2006/123/EC (on services in the internal market); Directive 2002/58/EC (processing of personal data and the protection of privacy in the electronic communications sector); the proposed Consumer Rights Directive; proposed Council and Parliament Decision to ensure mutual recognition of e-identification and e-authentication across the EU based on online 'authentication services' to be offered in all Member States; and Directive 2009/136/EC which is the EU Cookies Directive for users to 'opt in' (JRC 2012: pp. 95-96).

disclosed and multiple electronic identities managed. About three in four respondents reported to accept revealing personal data online as a common practice. For example, people disclose biographical data like a name to access a certain service, address and financial information in case of purchases.

The study also found that respondents – particularly, older or more active ones - are aware of the risks of making online transactions. In the context of eCommerce, some 30% of the respondents said that they did not have any control over their disclosed data. They attempt to protect their data by using tools like anti-spam software. Some 90% of the respondents said to "favor equal protection of their data protection rights across the EU, even though a majority feel responsible themselves for the safe handling of their personal data" (p. 15). In terms of trust, respondents tend to trust (medical) institutions with their data, less so governments and banks but far more than companies. Moreover, most respondents had a liking to the main principles of existing European Data Protection[3] legislation that is concerned with homogeneous and cross-border data protection rights among member states, notifications in case of lost/stolen personal data, and the ability to remove or edit personal data at any given point in time (cf. ENISA 2011).

The findings have also pointed to an interest to coming up with technical solutions or systems to address certain issues such as 'trust portability' from public to commercial contexts facilitated by credentials provided or supported by the government, "a disclosure system based on third-party credentials, and other ways of pegging 'virtual identity' to real identity", and "interoperable, easy to use national and cross-border systems with similar looks and feel" (p. 18).

In view of this, member states were urged to coordinate efforts in electronic identity (eID) activities. One effort in this direction is STORK[4] that works towards the implementation of an EU wide interoperable system for recognition of eID and authentication allowing the usage of national electronic identities across member states. Most national identity management (IdM) strategies tend to be evolutionary rather than revolutionary, that is, extend on existing offline practices and frameworks (OECD 2011).

---

[3] In the EU Data Protection Directive (95/46/EC) personal data "shall mean any information relating to an identified or identifiable natural person ('Data Subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity." See http://www.dataprotection.ie/viewdoc.asp?DocID=92

[4] See https://www.eid-stork.eu/ Also, see http://www.eid-ssedic.eu that offers a platform for all stakeholders of eID in support of a proposed Single European Digital Identity Community as foreseen by the Digital Agenda (EC). See also http://www.tas3.eu/ for a trusted architecture and set of adaptive security services that aims at preserving personal privacy and confidentiality in dynamic environments.

From privacy by design to 'protected sharing by design'

Accepting this line of findings, a move can be distilled towards self-regulation and 'privacy by design' (PbD) solutions (JRC 2012: 24). This principle allows for anonymous and pseudonymous interactions and transactions rather than the receipt of someone's extensive identity information. More specifically, PbD should prevent privacy risks before they materialize, privacy should be by default - a fundamental right, embedded in IT systems, fully functioning, secure and transparent.

PbD advances the view that the future of privacy cannot be assured solely by compliance with regulatory frameworks; rather, privacy assurances must ideally become an organization's default mode of operation.[5] In 2010 the European Data Protection Supervisor (EDPS) proposed the EC to embed PbD on different levels of law and policy making. It advised, among others, to have the PbD principle guide the Digital Agenda[6] and to include PbD in the legal framework for data protection.[7]

Yet, as was mentioned earlier, data are extremely powerful in political and economic terms, thereby highlighting risks that result from unprotected and unwanted disclosure and from a lack of sharing and use. In fact, a failure to anticipate and treat such problems can be detected calling for a system that provides need services and interventions, allows for discovery and innovation, and necessary coordination of complex organizational processes.

In this view, there is not just a need for PbD but rather a 'protected sharing by design' (PSbD), a highly scalable means by which there are the right balance of incentives and penalties to share, protect, and innovate in data services. The model for this is a so-called 'Trust Framework' which is a "combination of software mechanisms, legal contracts and social rules. Together these integrated elements set forth an algorithmic 'constitutional system' of governance and enforcement for a given body of information and people who use it. The trust framework constitutes a voluntary 'social contract' governing how that body of information may be shared and used in specific contexts."[8]

Approach; urban trust framework

The challenge is thus to provide a (legal) framework that is supportive of this new approach to privacy and identity and which can encourage innovation and

---

[5] See also http://privacybydesign.ca/

[6] See http://ec.europa.eu/information_society/digital-agenda/index_en.htm

[7] See http://EDPS-2010-06_Privacy in digital age_EN.pdf

[8] See http://idcubed.org/vision/what-is-a-trust-framework

And, rather than a government-produced (or supported) eID per se it is recommended to form a government sanctioned trust framework (such as ICAM in the US) for identity services. In this, the government is not a provider of identity services, but rather sets standards for private vendors who are in turn certified by, in the US case, the Open Identity Exchange.

adaptation while 'reinventing' the notion of privacy in the context of rapid and fundamental technological innovations. Without strong governing principles, a willingness to let market acceptance alone define norms or expectations of privacy could fundamentally undermine democratic principles. If people could be enticed to relinquish their privacy rights in exchange for financial and other incentives, and if governments and corporations could form their own surveillance and behavior monitoring networks at will, then citizenry would over time be relinquishing their autonomy and democratic powers to the government or other entities. Hence, a viable notion of digital privacy requires a digital form of effective democratic governance whereby not only public institutions but private ones as well are accountable to principles of fairness, choice, dignity, transparency and public welfare.

Fortunately, there is a growing recognition among significant policy makers in the US and the EU to develop new approaches to protecting and sharing private information that embodies a more open platform and ecological approach. The differences between this more holistic and evolutionary approach and the more classic mechanistic models of the past are significant and have broad implications on how to frame, oversee and implement complex regulatory policies.

We would propose a trust framework as it allows for a different way of framing of the problem by devising an acceptable systemic and evolving solution for users, vendors and regulators alike. It reframes the question to the extent one can trust a service to protect and share their personal information in a way that not only does not harm them but also helps them and the public realizes the greatest value of that information. In such a kind of identity ecosystem different players can be trusted to act not only in their own interest but also of other stakeholders. Trust is thus not 'blind' but rather verifiable holding different parties accountable through audits, mechanisms and enforceable agreements, and which is underpinned by a combination of architectural principles, methods of authentication, protection, encryption, permissioning and governance principles, contracts, and mechanisms for defining harms and remedies, adjudication and enforcement.

In the context of urban infrastructures, municipalities or sovereign regions need to have an open means to assert oversight over how data are being captured, shared, used, and monetized and, thereby, define and enforce agreements for the trusted exchange of data. They should also be in a position to manage the risks of data sharing and set transparent and enforceable criteria of performance for all members of a trust framework. They should be able to set the contractual terms for participating parities; set the criteria of performance, audits, dispute resolution, penalties and enforcement. They should not become locked into proprietary systems or vendors. And, governance and privacy should not be done as an after thought rather it has to be built in from the very beginning.

An urban trust framework is systemic and open allowing for the interoperability of data among different jurisdictions. In doing so, it allows for a minimum of friction in

making and evolving changes – making it modular and symmetrical with no privilege to any one part or member of a trust framework; for organizing it to innovate to drive down or commoditize costs; and for the provision of fundamental service innovations across sectors. For this to work certain design and governance principles (and metrics) will need to be established. Thereby it is important to establish what should be done within the trust framework and what not.

An urban trust framework, for example, could consists of a set of individuals and organizations and 'apps' that interact with one another and are involved in a variety of kinds of data exchange (and, rather than self-created user profiles, logins and other data, as most traditional apps do, these apps could for instance access personal data about the individual from the individual's Personal Data Store (PDS) (cf. Higgins Project;[9] WEF 2011). Each app itself should governed by a trust framework policy that provides a legal framework and operating rules for the behavior of the app, what kinds of data the app has access to, what the app is allowed to do with these data, and so on.

The individual members would be equipped with their own PDS and associated Websites and devices/PCs, with the individual's own data rendered. Other 'members' such as organizations of the network could offer Web services (such as in the case of EPIC, relocation services). All of these services could be governed by, for example, an 'open governance platform', and in this case, maintained by the city. Thus, organizations such as social networks, telcos, banks, data brokers, merchants, associations, etc. could offer Web services that are governed by the platform. So, the city and its neighborhoods could assist retailers, civic organizations et cetera in the delivery of urban services and let them develop the apps within the urban trust framework.

Cities could control large portions of apps in support of the city, and make them free (or small fee, e.g. 'chargeable app') and open supported by personal data lockers, authentication, discovery services, offer services, registration of apps, payment and digital currency systems, audit and audit criteria, dispute resolution. The city could be the provider of some kinds of services and originator of some kinds of data such as from sensors, transport, education and government services, and which could be used by individuals and private companies.

The value and revenue flows will depend of the kinds of producers, consumers, data miners, auditors etc of different data driven services as well as how they might be overseen such as by a trust agreement and card issuers with possible fees to different parties including individuals, governments and civic institutions or groups. Not the particular implementations should be regulated or how to prevent harms but rather what the harms could be and whether they have been prevented or to what level of risk and incidence.

---

[9] See http://eclipse.org/higgins/

In doing so, data get secured, connected and empower users.

Acknowledgments
The authors would like to acknowledge IBBT-SMIT, Vrije Universiteit Brussels and EPIC (the research leading to these results have received funding from the European Union Competititveness and Innovation Framework Programme 2007-2013 under grant agreement n° 270895). We also thank Bethan Allen for her assistance.

References
- boyd, d. and Crawford, K. (2011). "Six provocations for big data." Paper presented at the Oxford Internet Institute Decade in Internet Time Symposium, September 22. See http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1926431 (accessed 13 July 2012).
- ENISA (2011). “Privacy, accountability and trust – Challenges and opportunities”, *ENISA Reports*, February. See http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/pat-study (accessed 13 March 2012).
- Holland, R. (2005). “Will the real smart city stand up?”, *City*, 12, (3), pp. 302-320.
- JRC (2012). “Pan-European survey of practices, attitudes and policy preferences as regards personal identity data management”, European Commission, Joint Research Centre: Institute for Prospective Technological Studies. See http://is.jrc.europa.eu/pages/TFS/documents/EIDSurvey_Web_001.pdf (accessed 21 July 2012).
- OECD (2011). “National strategies and policies for digital identity management in OECD countries”, *OECD Digital Economy Papers*, No. 177, OECD Publishing. See http://dx.doi/org/10.1787/5kgdzvn5rfs2-en (accessed 14 January 2012).
- WEF (2011). “Personal data: The emergency of a new asset class”. See http://www.weforum.org/personaldata (accessed 13 February 2012).