PICASSO POLICY BRIEFING (updated)

Identifying horizontal policy issues in ICT

On January 1st, 2016, the project PICASSO was launched with the aim (1) to reinforce EU-US collaboration in ICT research and innovation focusing on the pre-competitive research in key enabling technologies related to societal challenges - 5G Networks, Big Data, Internet of Things and Cyber Physical Systems, and (2) to support the EU-US ICT policy dialogue related to these domains by contributions related to e.g. privacy, security, internet governance, interoperability, ethics.

PICASSO is oriented to industrial needs and provides a forum for ICT communities. It is building on a group of 24 EU and US committed prominent specialists in the three technology-oriented ICT Expert Groups and an ICT Policy Expert Group, working closely together to identify policy gaps in the technology domains and to recommend measures to stimulate the policy dialogue in these areas. This synergy between experts in ICT policies and in the three ICT technology areas is a unique feature of PICASSO.

During its first meeting on 20 May 2016 in Washington DC, hosted by NIST at the Department of Commerce, PICASSO experts and other experts in the field will focus on identifying the key issues in each specific field (5G, Big Data, IoT/CPS) and on policy issues that touch upon all of these domains. The ICT Policy Expert group will focus on Privacy and Data Protection, in recognition that policy issues relating to this touch all PICASSO related ICT developments across the Atlantic.

This briefing is meant to provide a starting point for all expert groups, expressing an invitation to the three specific expert groups (5G, Big Data, IoT/CPS) to reflect upon relevant policy issues, and to reflect specifically on how Privacy and Data Protection touch their specific domain.

All this is input to a series of 5 thematic Policy Papers and accompanying Webinars that are to take place over the coming two years. The intent is to get a clear overview of the priority policy issues in ICT collaboration – related to PICASSO domains, and insights in how these issues can be addressed from a bilateral multistakeholder perspective in a global context.

Currently, we identified the following candidate policy issues as input to PICASSO expert group reflections: <1> addressing global societal challenges “respecting Human Rights”; “Climate Change (COP21)” ;“supporting Sustainable Development Goals (SDGs)”; <2> “trust and confidence”; “encryption”; “censorship”; “surveillance”; “security”; “anonymity”; <3> innovation ecosystem: “startups”; “incubators”; “accompanying measures”; <4> (open) standards, certification, transparency & choice. These possible policy subjects are provided as a starting point, and may or may not end up as one of the 5 focus policy issues to be discussed in PICASSO, depending on the opinion of the PICASSO expert groups re: relevance to their specific domain. More specific thoughts on the issues that *is* identified as subject for the first policy issue, Privacy and Data Protection, are attached to this letter as initial briefing.

Please feel free to share your thoughts via email to maarten@gnksconsult.com.
Looking forward to engaging with you all,
Best regards

Maarten Botterman
Chairman Policy Expert Group
PICASSO project

Dave Farber
Co-Chair Policy Expert Group
PICASSO project

PRIVACY AND DATA PROTECTION
and its impact on EU/US ICT Policy collaboration

One of the objectives of the PICASSO project is to bring forward policy recommendations that are designed to improve the EU/US ICT collaboration, specifically in the areas of 5G networks, Big Data, and IoT/CPS. One of the most contested issues across the board is personal data privacy, which is not only a matter of concern to private sector and civil society stakeholders, but is also an increasing bone of contention between national and supranational governments in relation to criminal justice, national security and other vital national interests.

Whereas PICASSO will not be able to satisfy all concerns across all stakeholders, the aim will be to explore how US/EU collaboration in ICT can be served, best, taking into account the differences in approach towards privacy and data protection in the USA and in Europe, with respect for law and citizens' expectations, as well as the approaches by industry towards benefiting from the new opportunities, and keeping the widest possible space for innovation and deployment.

In addition to being an important topic in its own right, privacy and data protection issues complicate trade negotiations, freedom of information rules, digital rights, intellectual property protection and financial regulation. With particular reference to the transatlantic dimension and the specific PICASSO domains of 5G networks, Big Data, and IoT/CPS, it features in the evolving arrangements over corporations' personal data collection, storage, processing and access (on one side the EU-US Privacy Shield, which tends to restrain businesses, and on the other those provisions in TTIP, TPP and especially TSIA that effectively protect corporations from government restraint). Beyond this direct consideration of transatlantic data flows are indirect tensions arising from divergent legislative and legal developments, such as US moves to limit government powers to compel businesses to provide access to personal data (especially bulk phone records) e.g. in the USA Freedom Act contrasted with the enhanced powers over acquisition of communications data, interception of communications, bulk personal datasets and equipment interference detailed in the UK's proposed Investigatory Powers Bill and the accompanying Code of Practice[1]. These raise a range of thorny questions, including the extent to which Europe's data protection apparatus reflects a legitimate regional ethical stance (privacy as a fundamental rather than an economic right) rather than a protectionist barrier to commerce and a hindrance to economic growth[2].

The context for these developments – and a major potential stumbling block or opportunity is provided by the complex and very different framing and legal status of privacy both between the US and Europe and within Europe. The EU tends (with some Member State and data type exceptions) to view data privacy as a *fundamental* right independent of founding documents such as the TFEU)[3]. The US tends towards an *economic* right interpretation deriving explicitly from a Constitutional base. The EU applies privacy protections to *broad classes* of data collection and handling (in the General Privacy Regulation which will come into force in 2018), while the US protects only *specific types* of data (e.g. health-related and financial, see below). The EU has only recently

[1] For the Bill and Codes of practice, see https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/473770/Draft_Investigatory_Powers_Bill.pdf and https://www.gov.uk/government/publications/investigatory-powers-bill-codes-of-practice.

[2] As Carl Bildt of the Global Commission on Internet Governance put it: "Barriers against the free flow of data are, in effect, barriers against trade." Cf. http://www.ft.com/cms/s/0/5d626a4e-f182-11e4-88b0-00144feab7de.html#axzz3fad5AuLJ.

[3] This is explicitly reflected in the recent European Court of Justice ruling invalidating the Safe Harbour Agreement on the grounds of incompatibility with "fundamental rights and freedoms, notably the right to privacy" (cf. http://static.ow.ly/docs/schrems_3OHQ.pdf.

framed a *general Right of Erasure*[4] - its exercise is a responsibility of data subjects and liability for complying remains with data controllers. By contrast, the US *mandates erasure of specific data*[5]. The EU focuses on protecting citizens against *data privacy* invasion by *private sector actors*, while the US Constitution's Fourth Amendment protects citizens against "unreasonable search and seizure" *by government* and has (through Supreme Court decisions) used the Due Process clause of the Fourth Amendment to recognise 'unenumerated' or shadow privacy rights that go well *beyond mere data protection*. Another difference is the largely negative cast of US rights, which *prohibit* government from taking certain actions against its citizens compared with the EU framework's addition of 'affirmative' provisions *requiring government actively to protect rights* against infringements by other actors.

The net result of these differences is a tendency for US negotiators to treat privacy primarily as a trade issue, while their EU counterparts see the issue as necessarily going well beyond commercial or economic considerations and mechanisms. Even mutual recognition does not necessarily provide a starting point for agreement, as 'mutuality' is so hard to define.

There are opportunities as well. Different approaches can reveal latent preferences such as the appetite of US consumers for anonymous profiling tools developed to protect data subjects while making their data suitable for economic use. The use of different approaches despite roughly similar technologies, services and business models creates an ideal natural experiment to help separate essential from inertial aspects of privacy and to point the way to suitable 'bridging' frameworks.

Such questions have been complicated by technological and societal changes linked to the spread of ICTs. Examples include: the difficulty of separating the private data of multiple individuals across national borders in order to establish the limits of commercial exploitation and government access; the extent and nature of privacy threats and protections connected with the Internet of Things; the status of data storage and processing facilities used in cloud computing; the implications of data protection rules for (big or small) data analytics and the commercial and legal implications of encryption in communications and storage.

To explore these issues with a focus on the specific domains of 5G networks; Big Data; and IoT/CPS, it is useful to re-examine the operational meanings of all three words in the term 'personal data privacy'

- *Personal* normally means the legal, natural and intentional aspects of individual human beings, but may need to be broadened or stratified to consider e.g. the degree to which on-line or automated associations result in shared identities and the extent to which 'protected' personal information does not originate with the person but is attached to them by e.g. governments, businesses or on-line choices framed and monitored by (often-invisible) third parties (like clickstreams). If by 'person' we mean an entity that reveals and uses data to make decisions and take actions, we must adapt our governance arrangements to cope with actors who may be non-human (e.g. the sensors and actuators of the IoT), non-physical (e.g. algorithms) or even non-unique (e.g. complex interacting networks of people, things and scraps of code). Therefore, as new technologies and natural processes such as ageing limit the reliability or even the feasibility of informed consent for 'natural persons' and important behaviour moves away from the narrowest definition, the 'person' may no longer be a source of reliable normative authority or control. WHAT ABOUT "NATURAL PERSON"?
- *Data* normally means records, and increasingly must be distinguished from information or the results of processing. In particular, the right to insist that data are correct, in addition to being almost prohibitively costly and time-consuming, does not protect data subjects from incorrect or damaging consequences based on subsets of data or their combination with other, non-personal data. Beyond

[4] See Articles 17 and 19 of the General Data Protection Regulation – note that Article 17(2) requires data controllers to notify third-party processors that an erasure request has been made, and makes them liable. See text at: http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2014-0212&language=EN.

[5] E.g. health data - HIPAA (Health Insurance Portability and Accountability Act) and financial data - FACTA (The Fair and Accurate Credit Transactions Act of 2003); GLB (Gramm-Leach Bliley); Sarbanes-Oxley Act (SOx); and Payment Card Industry Data Security Standards (PCI DSS).

this, the protection of data may be far less important than the protection of individuals from unwarranted interference with their right to choose actions and give consent and the protection of 'authoritative' or durable data may become less important than protection of individuals from harms arising from exploitation of ephemeral data.

- *Privacy* – is continually being redefined (e.g. as a fundamental or an economic right, or as something the state, as opposed to the individual, provides and protects). As these definitions change, systems of law and practice based on them may diverge, creating new problems. If it is not possible to devise an acceptable future-proof definition, it may be useful to recast privacy in terms of *access* to information, data and opportunities to act and *responsibility* for the consequences of having or using such access. In this way, the relation between privacy and equally-nuanced concepts like security becomes less a matter of dichotomy than of spectral dispersal (i.e. a range rather than a point).

The time seems right for a proper, transatlantic (in the first instance) dialogue on the consistency of national and international privacy arrangements and the internal consistency of national approaches to privacy that differentially affect the interests of people and companies from the other side of the ocean. In this, PICASSO will focus on the specific aspects touching upon the development and deployment of 5G networks, Big Data, and IoT/CPS.

In DC we will be looking for examples of privacy challenges that are barriers for collaboration, or, indeed, opportunities for collaboration where technology could help resolve challenges. The emphasis of our search for answers is on ways forward that allow ICT related products and services from both continents to be used at both sides of the Atlantic – and how collaborating researchers from EU and US can effectively make this happen.

This paper is input to the meetings that are hosted by NIST in DC on 20 May 2016, and as such a first step in developing a policy paper on this topic. In the policy paper, we aim to include specific examples related to 5G Networks; Big Data; and IoT/CPS.

Agenda for 20 May 2016

For all PICASSO expert groups, the request is to consider, with regards to Privacy and Data Protection and specifically from the perspective of your specific area of expertise:

1- In what way touch privacy and data protection upon EU-US collaboration in your domain? Please list both barriers and opportunities.

2- What other EU and/or US policy issues have an important impact on EU-US collaboration in your domain? Please list the policy issues identified, and the related barriers and opportunities.

THANK YOU FOR YOUR CONSIDERATION. TOGETHER, WE CAN IMPROVE US/EU COLLABORATION IN ICT THROUGH BETTER POLICIES AND EFFECTIVE POLICY SUPPORT.