PICASSO POLICY BRIEFING 1 (draft input to webinar)

Privacy and Data Protection Issues Affecting EU-US ICT Collaboration

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

PICASSO is oriented to industrial perspectives and provides a forum for ICT communities. It is built around a group of 24 EU and US specialists, organised into the three technology-oriented ICT Expert Groups and an ICT Policy Expert Group and working closely together to identify policy gaps in or related to the technology domains and to recommend measures to stimulate policy dialogue. This synergy among 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 the Department of Commerce, PICASSO experts and other experts focused on identifying key issues in each focus technology area (5G, Big Data, IoT/CPS) and on those policy issues that influence and are influenced by all of these domains. In its first meeting, the ICT Policy Expert group focused on Privacy and Data Protection, recognising that these issues are entangled with all PICASSO-related ICT developments across the Atlantic, directly affecting ICT collaboration. Whereas technology can help addressing policy/societal challenges in ways that have not been possible before, it also poses new challenges for policy/society that need to be considered. In particular the real and perceived policy differences between the EU and USA may make it more difficult for ICT researchers to collaborate towards technology and technology deployment solutions that are suitable for both US and EU markets. In this, there is a role for commerce, business and the economy, since economic methods and motives drive both policy and technology, as well as provide their own forms of problems and solutions.

Amongst its activities, the PICASSO Policy Expert Group is organising a series of webinar to share its reflection with selected experts. The present briefing is meant to provide input for a first webinar, inviting all three thematic expert groups (5G, Big Data, IoT/CPS) to join us in reflecting upon the reciprocal impacts of privacy and data protection on their specific areas of expertise.

This is the first of 5 thematic Policy Papers and accompanying Webinars that will take place over the coming two years. Future subjects for Policy Papers will be Security; Standardisation; Spectrum; and one to be decided – currently “Smart Cities”. The intent is to get a clear overview of the most pressing and/or challenging policy issues that confront technological, business and policy collaborations, and to develop valid and practical insights into how these can be addressed from a transatlantic multistakeholder perspective operating in a global context.

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

PICASSO has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement N° 687874.

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

One objective of the PICASSO project is to bring forward policy recommendations designed to improve EU/US ICT-orientated collaborations, specifically in the technological domains associated with 5G networks, Big Data, and IoT/CPS. One of the most contested issue sets across the board concerns personal data protection and privacy (closely related to each other but not at all the same thing). This pair of issues is not only a matter of concern to the private sector and to civil society, but is also an increasingly-fraught bone of contention in the government sphere, where national governments and supranational governance entities tussle over criminal justice, national security and other vital national interests.

These technological domains overlap in the technological, economic/commercial, business and societal planes. Each of these dimensions creates a shared perspective on the common problems and thereby serves as a platform for internal as well as cross-plane (multistakeholder) interaction. Problems, issues or challenges may have their causes in one (set of) planes, their effects in another and their solutions in a third. Therefore, the interactions (here called 'collaborations') combine collaboration with competition. Concretely, privacy issues can be resolved by various technological, economic and policy measures, or by the evolution of societal norms adapted to the modern technological and economic dimensions of privacy (e.g. as the possibilities for infringing privacy and the value of doing so change, the bounds of acceptable behaviour and the sanctions for violating them also change). Whether EU/US collaboration leads to a technological, economic, regulatory or societal 'solution' will depend on a competitive struggle (across markets, labs and legislatures) as much as it does on a cooperative, neutral and civilised discussion. This mix of modes (cooperation, competition and conflict) can clearly be seen in e.g. TTIP and Privacy Shield.

Although PICASSO will not be able to fully address all stakeholder concerns, it aims to explore how US/EU collaboration in ICT can best be served, taking into account the differences in approach towards privacy and data protection in the USA and in Europe, respecting the law and citizens' expectations and preserving the widest possible scope for innovation and deployment.

This paper is based on the policy briefing on Privacy and Data Protection to the PICASSO ICT Policy Expert Group, prepared for meeting hosted by NIST in Washington DC on 20 May 2016 and the following discussion in this Group. Subsequently, the paper has been updated with recent developments and serve now as input to the first Policy PICASSO webinar that will be held on 11 October 2016 (starting at 15:00 UTC).

In essence, the call is for consideration of a privacy taxonomy within each of the three PICASSO domains for EU-US ICT collaboration, and for recognition of the need to build in an ethical approach in product innovation, development and deployment recognising that the issues are global and can only be addressed in a multistakeholder way; and for transparency on the use of personal data in applications and of accountability of actors in the value chain.

Summary of Discussion so far

In addition to being important topics in their own right, privacy and data protection affect many different sectors, complicating negotiation and rulemaking on trade, freedom of information, digital rights, intellectual property and financial services. With particular reference to the transatlantic dimension and the specific PICASSO technological domains (5G networks, Big Data and IoT/CPS), they feature prominently in the evolving (or disintegrating) arrangements over corporate and government processing (collection, storage, processing, access etc.) of personal data. As regards corporate processing, these arrangements run the gamut from the EU-US Privacy Shield, which tends to restrain businesses, to those provisions in TTIP, TPP and especially TSIA that effectively protect corporations from government restraint. Beyond such direct attempts to tackle transatlantic data flows are indirect tensions arising from divergent legislative and legal developments. This can be seen in

PICASSO has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement N° 687874.

the recent flurry of activity regarding surveillance and especially the exercise of so-called 'bulk powers[1]' around which different governments appear *not* to be converging, yet[2].

A framework for collaboration needs fully to reflect our shared democratic and individual rights-based values, expressed on the EU side by the Lisbon Treaty and the Charter of Fundamental Rights, and on the U.S. side by the U.S. Constitution. They also, inevitably need to reflect the differences that enrich our interaction.

At this stage, the main conclusions are:

- Privacy and interoperability of systems are opposite sides of the same invaluable coin. Participants agreed that it would be important for industry to explicitly consider the human element from the outset when developing industrial solutions;
- The awareness of policy makers, citizens, consumers and the commercial world of what is technologically possible, economically advantageous, socially acceptable, politically viable, legally allowed and ethical could usefully be raised. It was agreed that those with important decisions to make and those most exposed to the consequences too often only have limited insight into what is happening on the ground.

Fundamental questions need to be answered to understand the real scope of the challenges to collaboration in these areas. In what sense can we say to have, want or need privacy? We have witnessed massive disclosures and debates on the level and kind of surveillance that is "proportional". Furthermore, it is clear that the Internet (and many information systems) today is not build to be secure, let alone secure in operation, which raises the questions: is security always a good thing, and what *can* we do when things are not secure? For instance: over-reliance on system security may lead to crowding out of efficient or sensible precautions which causes greater security pressures on systems and the danger of dwindling awareness of security or unbalanced consideration of risks.

Knowing that we rely on a rapidly growing and increasingly difficult to comprehend or control base of hardware and software to facilitate our societies, how do we survive in a world built on billions of machines created in another time and insecure by default, design or development, which are not going to simplify or disappear? This has to be considered at some point, and sooner rather than later. Otherwise, we risk a reality that we cannot perceive, let alone deal with.

Taxonomy: part of the answer to the search for clarity

There was a call for a taxonomy of "privacy sensitivity" of different categories of 5G/IoT/Big Data applications. This because the potential privacy impact of different applications and how they are used varies greatly, from "trivial" to huge, and from positive to negative. It was further pointed out that a taxonomy for privacy should form part of a joint taxonomy with "security" and "safety" dimensions, understanding that these issues overlap.

In this, it is important to distinct between static and dynamic notions of privacy, security and safety. The static notion refers to today's situation and protections; the dynamic situation refers to innovation and development. A deficiency in one is generally linked to an advance in the other. This has a transatlantic aspect related to differences in emphasis in competition policy between the EU and the US, as in the US in general emphasis is put on allocational efficiency, whereas in in Europe there is more emphasis on dynamic and societal efficiency.

This would help identify areas and distinguish 'technology-led' areas where further EU-US collaborative and competitive ICT innovation should charge ahead at full steam without being held back by privacy and data protection issues, from 'policy-led' areas where incompatibilities between EU and US approaches or 'wicked

[1] These include: **interception** of communications (intercepting communications as they travel across networks); **equipment interference** (acquisition of communications and equipment data directly from computer equipment); **communications data** (obtained from communications service providers); and **personal datasets** (e.g. travel data or Government databases).

[2] e.g. the USA Freedom Act, the UK Investigatory Powers Bill and the EU's Data Retention Directive (2006/24, overturned in 2014) and Police Directive (2016/680).

PICASSO has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement N° 687874.

issues' that require joint political clarification must be tackled first in order to set the guidelines and (legislative and other) framework conditions within which technological and market-facing cooperative and competitive innovation can be pursued. In this it is important to consider both areas where the impacts are trivial or uniformly positive and areas where the privacy, security and safety implications need to be sorted out after the technology is understood, and not before, because technology and its use may reshape or reframe the issues. For instance, the advent of evanescent communications technologies ranging from Instagram/SnapChat to cc. mail have completely rewritten the ground rules of communications data privacy, meaning that the problem, objectives, options and impacts all need to be rethought rather than restored.

Independently from the answers to the above questions, experts agreed that privacy and data protection in both the EU and the US would be enhanced if the following principles were followed in ICT innovation and development:

- Transparency: people must (be able to) understand how their environment affects data protection and privacy. In particular, it is necessary to develop clear and suitably-refined notions of data ownership and control, to identify who controls what, which data are processed, in what way and for what purpose(s). Transparency is also necessary to be able to monitor what is going on at the level needed to enforce agreed rules and norms. And in order to be able to deal with complexity, (trusted) technology may help to create transparency;
- Accountability: Rules and norms cannot be enforced if lines of accountability are unclear, since it is not possible to know whom to call to account, on whom to impose liability and to whom to delegate authority or the power to act. With suitable accountability, however, self-enforcing mechanisms can be designed or evolve to keep actors from damaging each other, on the basis of clear constitutional principles, and establishing levels of good practice will help ensure establishing "what can be expected" as "proper care" by a service providers;
- Context: consumers, citizens and others whose choices determine market outcomes should not be surprised or misled … requires interoperability, security, standards, etc.
    - Joint taxonomy of the privacy, security and safety sensitivity of different categories of 5G/IoT/Big Data applications; and
    - technical standardisation processes that are built on clear ethical principles, using informed consent where appropriate and feasible and taking ethical considerations into account such as from the IETF Privacy considerations RFC "ask yourself …"

Background

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[3]. 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

[3] 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.

PICASSO has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement N° 687874.

rather than an economic right) rather than a protectionist barrier to commerce and a hindrance to economic growth[4].

Differences in legal status of privacy

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)[5]. 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 framed a *general Right of Erasure*[6] - 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*[7]. 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. Also recognising that a taxonomy would help to identify those areas where the differences in approach do not affect the ability for EU-US ICT collaboration, and creating such a taxonomy, could potentially be hugely beneficial.

Current legal environment

More and more emphasis has been put by citizens/consumers on privacy in an increasing digital world. Awareness is raising, although few people today are well informed about the real issues, and anecdotal research demonstrates time and time again that the "costs of privacy" vary greatly depending what is on offer.

[4] 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.

[5] 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.

[6] 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.

[7] 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).

PICASSO has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement N° 687874.

As said in the introduction: the basis for legislative protection of data and privacy is different in the US and In Europe: so is the legislative approach. At EU the basis can be found in the Lisbon Treaty and the Charter of Fundamental Rights and on the U.S. side in the U.S. Constitution.

EU legislation has been moving recently from its original guidance by the Data Protection Directive of 1995 (further: DPD) towards the General Data Protection Regulation which will be fully in force by May 2018 (further: GDPR), thus to allow European Member States to adjust their national legislation that was put in place pursuant the DPD towards the now European level legislation. US legislation regarding to data protection is merely sectoral and subject to individual Court's Decisions (Case Law). Both the EU and US developing frameworks are described below.

Europe: the General Data Protection Regulation

When the original Data Protection Directive was developed and agreed in 1995, the Internet was by far not as important as today, and nobody had even mentioned the term "Internet of Things" yet. A review of the 1995 Directive in 2009, sponsored by the UK Data Privacy Authority, already noted that new developments like IoT, data mashups and data virtualization are new challenges that had to be met[8]. The reform that led to the new General Data Protection Regulation (further: GDPR) has been under way since 2011 and culminated in a Proposal to Council and Parliament by the European Commission on 25 January 2012. This proposal was approved by the European Parliament in March 2014, and has now been finalized and ratified by Parliament and Council to come into force in May 2018.

With this, it should be noted that the work has not been completed. When this law was set up in outline in 2011, "Big Data" was not yet an issue widely recognized, in that year new in the Gartner Emerging Technologies Hype Cycle. Today, we know that big data, and big data analytics, fundamentally challenge the concept of "personal data" as through big data analytics data that in isolation do not relate to persons often can be related to persons when combined with other data. Published in 2014, the Opinion from WP29[9] on IoT recognised the value of IoT, as well as the potential intrusions it can generate to privacy. Future developments in increasing abilities and new ways of using technologies and data will continue to be considered in the light of the current Legislative framework.

USA: Case Law based on the Constitution[10]

The US has no single data protection law comparable to the EU's Data Protection Regulation. In the US privacy legislation has developed on an *ad hoc* basis when required by certain sectors and circumstances. Fundamental within the US is "The Fourteenth Amendment (Amendment XIV)" which was adopted in the United States Constitution on July 9, 1868. The Amendment addresses citizenship rights and equal protection of the laws, and was proposed in response to issues related to former slaves following the American Civil War. The first section of The Fourteenth Amendment is one of the most litigated parts of the Constitution and has been used as the basis or a number of landmark decisions, e.g. such as Roe vs. Wade (1973) regarding abortion, Bush vs. Gore (2000) regarding the 2000 presidential election, and Obergefell vs. Hodges (2015) regarding same-sex marriage. Critically the amendment limits the actions of all state and local officials, including those acting on behalf of officials.

The right to privacy or the "right to be left alone" is a key area within the US. While not explicitly stated in the U.S. Constitution, some of the amendments provide a degree of protection towards privacy. Privacy is most often protected by statutory law in the US. For example the Health Information Portability and Accountability Act (HIPAA) protects a person's health information, and the Federal Trade Commission (FTC) enforces the right to privacy in various privacy policies and privacy statements.

[8] Neil Robinson, Hans Graux, Maarten Botterman & Lorenzo Valeri. Review of the EU Data Protection Directive, prepared for the Information Commissioner's Office, TR-710-ICO. Cambridge, May 2009

[9] The Article 29 Data Protection Working Party was set up under the Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. It has advisory status and acts independently.

[10] Legal analysis from PICASSO Deliverable 1.3 *Panorama of ICT landscape in EU and US: ICT, Policies, regulations, programmes and networks in the EU and US*. Authors: Haydn Thompson and Daniela Ramos-Hernandez, THHINK – UK

PICASSO has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement N° 687874.

There is a challenge, however, when there is a need to balance privacy against the needs of public safety and improving the quality of life, in some ways comparable to legislation related to traffic safety such as seat-belt laws and motorcycle helmet requirements. Most Americans accept that government surveillance and collecting of personal information is necessary. The right to privacy often relates to the right to personal autonomy where an individual has the right to choose whether or not to engage in certain acts or have certain experiences. Several amendments to the U.S. Constitution have been used in varying degrees of success in determining a right to personal autonomy:

- The First Amendment protects the privacy of beliefs
- The Third Amendment protects the privacy of the home against the use of it for housing soldiers
- The Fourth Amendment protects privacy against unreasonable searches
- The Fifth Amendment protects against self-incrimination, which in turn protects the privacy of personal information
- The Ninth Amendment says that the "enumeration in the Constitution of certain rights shall not be construed to deny or disparage other rights retained by the people." This has been interpreted as justification for broadly reading the Bill of Rights to protect privacy in ways not specifically provided in the first eight amendments.

However, the right to privacy is most often cited in the Due Process Clause of the 14th Amendment, which states:

No state shall make or enforce any law which shall abridge the privileges or immunities of citizens of the United States; nor shall any state deprive any person of life, liberty, or property, without due process of law; nor deny to any person within its jurisdiction the equal protection of the laws.

The protections have been narrowly defined and are usually interpreted as only applying to family, marriage, motherhood, procreation and child rearing. The controversial *Roe v. Wade* case in 1972 case 142 established the right to privacy as fundamental, and required that any governmental infringement of that right had to be justified by a compelling state interest.

In the US a person has the right to determine what sort of information about them is collected and also how that information is to be used. In the marketplace this is enforced by laws intended to prevent deceptive practices and unfair competition. The Privacy Act of 1974 prevents unauthorised disclosure of personal information held by the federal government. A person has the right to review their own personal information, ask for corrections and be informed of any disclosures. This has also been imposed upon financial institutions in the Financial Monetization Act (1999) which requires financial institutions to provide their customers with an explanation of what kind of information is being collected and how it is being used. Safeguards are also required to protect customer information, e.g. the Fair Credit Reporting Act, protects personal financial information collected by credit reporting agencies. The act puts limits on who can access the information and requires agencies to have simple processes by which consumers can get their information, review it and make corrections.

Online privacy is also important in the US and Internet users can protect their privacy by taking actions that prevent the collection of information, for instance not to allow tracking cookies. Browsers and social media platforms, e.g. Facebook and Twitter, allow user selected privacy settings, from sharing everything to only sharing with friends. At a minimum level this can be only a name, gender and profile picture and increasingly citizens are aware that it is necessary to protect personally identifiable information to prevent identity theft.
Also within the US the Children's Online Privacy Protection Act (COPPA) enforces a parent's right to control what information websites collect about their children. In particular websites that target children younger than 13 or knowingly collect information from children must post information on their privacy policies and also get parental consent before collecting information from children. Parents can thus decide how such information can be collected.

As well as a right to privacy there is also a right to publicity. Here there is a right to control the use of his or her identity for commercial promotion. Unauthorised use of someone's name or likeness is recognised as an invasion of privacy. This is classed into 4 areas: intrusion, appropriation of name or likeness, unreasonable

PICASSO has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement N° 687874.

publicity and false light. For instance, if a company falsely uses a person's photo in an advert claiming that the person endorses a product, the person can file a lawsuit claiming misappropriation.

The Supreme Court in the US approaches the right to privacy and personal autonomy on a case-by-case basis. Notably public opinion is constantly changing regarding relationships and activities. The boundaries of personal privacy are also changing due to social media and a move towards "sharing." As a consequence the definition of the "right to privacy" is constantly subject to changing interpretation.

The EU/US agreement Privacy Shield

The international Safe Harbour Privacy Principles enabled some US companies to comply with privacy laws protecting European Union and Swiss citizens by self-certifying that they adhere to the 7 principles underlying the European Data Protection Directive without further need for a formal certification process as would have been required otherwise by the European Data Protection Directive related national legislations.

In 2015, a Court Ruling by the European Court of Justice in the case of Maximillian Schrems versus the Irish data protection commissioner regarding the right of Facebook to transfer data to servers located in the USA under the Safe Harbour scheme declared the Safe Harbour Decision invalid. Reason given was that the protections under the Safe Harbour scheme provided by the US Authorities had proven to be inadequate, in particular because "*the scheme is applicable solely to the United States undertakings which adhere to it, and United States public authorities are not themselves subject to it. Furthermore, national security, public interest and law enforcement requirements of the United States prevail over the safe harbour scheme, so that United States undertakings are bound to disregard, without limitation, the protective rules laid down by that scheme where they conflict with such requirements*" and because for non-US citizens there is no opportunity to redress: "*legislation not providing for any possibility for an individual to pursue legal remedies in order to have access to personal data relating to him, or to obtain the rectification or erasure of such data, compromises the essence of the fundamental right to effective judicial protection*".[11]

IoT providers and Big Data companies such as the globally popular "Nest" smart meters and smoke detectors, owned by Google, continued to refer to "Safe Harbour Agreement" protection of personal data as there was no immediate alternative[12]. The measures currently proposed by the European Commission to replace "Safe Harbour", known as "Privacy Shield"[13], were approved by the EU Member States representatives (Article 31 Committee) on 8 July 2016, following which the European Commission adopted the framework on 12 July 2016 and it went into effect the same day. It should also be noted that this new agreement has not been tested in Court, yet, and until this is done and ruled to be a "valid agreement" uncertainty about this new protection remains.

The way forward

Businesses are looking for guidance, as Big Data is a subject of interest to many, and companies around the world are looking into the opportunities offered by Big Data, data generation, collection, and analytics. IoT is a major driver in this, as "connected Things" will generated endless streams of data that will be captured and used. From a business opportunity point of view, uncertainty about acceptable arrangements under the developing privacy and data protection regulatory frameworks affects the willingness of investors to invest in projects that may be seen as "privacy sensitive" and subject to data protection rules (and fines). According to the European Data Protection Supervisor (EDPS) Peter Hustinx[14]: "*If Big Data operators want to be successful,*

[11] ECJ ruling in case C-362/14 Maximillian Schrems vs Data Protection Commissioner, 6 October 2015, see http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf

[12] https://nest.com/legal/privacy-statement-for-nest-products-and-services/

[13] The EU-U.S. Privacy Shield imposes stronger obligations on U.S. companies to protect Europeans' personal data and requires the U.S. to monitor and enforce more robustly, and cooperate more with European Data Protection Authorities. It also includes written commitments and assurance regarding access to data by public authorities.

[14] Peter Hustinx according to Mark Say in the article "Big data needs big guidance" in FT, December 29, 2014. Retrieved http://www.ft.com/cms/s/0/fab4bae8-7f88-11e4-86ee-00144feabdc0.html#axzz3O8I1GAvc on 2015.01.07

PICASSO has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement N° 687874.

they should … invest in good privacy and data protection, preferably at the design stages of their projects". With this, he recognises the importance of "soft law" at this point[15]. Investing in good privacy and data protection should be core in the innovation, development and deployment of IoT, and probably a pre-condition for European (co-)sponsored research. A way forward could include the habit/obligation of a Privacy Impact Assessment in every stage of design of new IoT products and services.

In the Opinion on Digital Ethics[16] published by his successor EDPS Giovanni Butarelli refers to Article 1 of the EU Charter of Fundamental Rights: '*Human dignity is inviolable. It must be respected and protected*.' From that position he further explains that: "*In today's digital environment, adherence to the law is not enough; we have to consider the ethical dimension of data processing*." It is in line with this that projects funded by the European Commission are looking very carefully at the issue of privacy protection and the idea of limiting the amount of information available to each entity. In general, the key issue to take into account while discussing privacy has to do with the integration of information from different sources. While a single stream of data might not contain enough information to invade the privacy of the user, it is recognized that the correlation and concurrence of information at an entity can lead to privacy considerations that were unthinkable only looking at the individual sources.

While the user is ultimately responsible for the data it allows to escape in the open, a modern individual that works and lives with current technologies cannot keep up with the types and amount of information being "leaked" by applications and websites. It is, therefore, for an individual virtually impossible to design privacy policies that are permissive enough to allow for services to work, while at the same time, restrictive enough that the privacy of the user is not compromised. Any specific harm or adverse consequence is the result of data, or their analytical product, passing through the control of three distinguishable classes of actor in the value chain[17]:

1. Data collectors, who may collect data from clearly private realms, from ambiguous situations, or data from the "public square," where privacy ‐ sensitive data may be latent and initially unrecognizable;
2. Data analyzers, who may aggregate data from many sources, and they may share data with other analyzers creating uses by bringing together algorithms and data sets in a large ‐ scale computational environment, which may lead to individuals being profiled by data fusion or statistical inference;
3. Users of analyzed data generally have a commercial relationship with analyzers; creating desirable economic and social outcomes, potentially producing actual adverse consequences or harms, when such occur.

As the complexity increases through technology, we will depend on technology to deal with it. It is crucial that automated and self-configuring solutions are offered that analyze the type and amount of information given away for a specific user and configure the appropriate number of policies to ensure that the level of security and privacy desired by the user is kept untouched. This goes beyond mere regulatory actions and require robust and flexible technology solutions that work under very different conditions, and that are backed by legislation to ensure that abuse of technologies or data is subject to redress and legal action.

Dynamics of technological and societal change

Continuous (and increasingly rapid) changes in technology and society linked to the spread of ICTs complicates framing the issues, and at the same time highlights the opportunities that EU-US ICT collaboration can bring. ICT has become global as ICT products and services are potentially used anywhere in the world, and increasingly with localisation of data, software and hardware at places independent from the geographic location of the user. Examples of challenges that this brings include:

[15] See also: Europe's policy options for a dynamic and trustworthy development of the Internet of Things, RAND, June 2013

[16] Opinion 4/2015, Towards a new digital ethics: Data, dignity and technology, EDPS, 11 September 2015

[17] Executive Office of the [USA] President PACT report: Big Data: Seizing Opportunities, Preserving Values (May 2014)

PICASSO has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement N° 687874.

- difficulty of separating the private data of multiple individuals across national borders in order to establish the limits of commercial exploitation and government access;
- extent and nature of privacy threats and protections connected with the Internet of Things;
- status of data storage and processing facilities used in cloud computing;
- 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.
- *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 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).

What does this mean for EU-US collaboration in the PICASSO domains?

Having a deeper understanding of where all this stands, and the dynamics that result from <a> the fundamental differences in legal basis; <b> the ongoing technological and societal changes, it becomes apparent that some elements would help create common grounds for EU-US ICT collaboration and, in fact, go beyond that as ICT innovation, development and deployment is truly global in most perspectives.

First, a ***fundamental discussion on privacy*** is needed and going on in societies around the world, in which the need for balance between private and public interests are weighted and discussed and answers will not be the same for each society, as there are differences in cultural values and legal frameworks. A discussion that does need to involve policy makers and citizens around the world as technologies such as those discussed within the PICASSO project rapidly spread and become a more fundamental element of the fabric of our societies every day. The only way to ensure EU-US collaboration in ICT helps this world evolving in a direction people want through is by recognising that ICT truly has a global impact and affects people, in whatever way, shape or form and thus should be transparent in its use, both in what it does and who is responsible for what in values chains that are facilitated by ICTs. Obviously recognising the (ongoing) need for such a societal debate and reflection of it in actions from all stakeholders involved, be it:

PICASSO has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement N° 687874.

- citizens becoming more aware of the issues and asking for "better" products and services (to businesses?), and protection (to governments?);
- businesses being aware of their corporate social responsibility as well as their interest in developing products and services that are sustainable (read: legal, and/or attracting consumers) in the long run
- government being aware of citizens needs and protecting the public interest while balancing that public interest against the private interests (note that in many aspects public interest and private interest aligns).

Second, it seems that a ***taxonomy of data privacy sensitivity*** could help identify subdomains in which EU-US ICT collaboration is less hampered than with other subdomains. Not every domain has a similar relation to private data. For instance:

- IoT/CPS includes systems in which humans do not participate, thus data relating to individuals are not collected at all, or only partially relating to people. One could think of different CPS that are *not* privacy and data protection sensitive:
  - networks of sensors that do not identify persons as systems such as a tsunami detection buoys network;
  - data using to operate an object such as a car or a plane, as long as data are not related to persons using the object that is a CPS in itself;
  - and there is more …
- Big Data as a broad concept make it possible to combine data from many different sources, and with enough "global data" cross-matched, patterns may become granular enough to identify individual persons even if that was never the intent of specific data collectors, even if within their collected set of data it would have been impossible to identify individuals with any accuracy. This can only be dealt with by ensuring algorithms are built in such a way that they do not identify individuals. And there is more…
- 5G may be the area that is least directly affected by Data Protection legislation, and it will need to consider availability of location data related to devices owned by individuals, protection of data stored on devices, transfer of data through 5G networks, etc. And there is more …

Conclusion

The call is for further consideration of a privacy taxonomy within each of the three PICASSO domains for EU-US ICT collaboration, and for recognition of the need to build in an ethical approach in product innovation, development and deployment recognising that the issues are global and can only be addressed in a multistakeholder way; and for transparency on the use of personal data in applications and of accountability of actors in the value chain.

Recognising that the challenges in the field of privacy and data protection also offers opportunities (for those who find the best ways to address them), it is up to the legislators to ensure "responsible innovation" is possible, so as not to stifle innovation and economic growth where that is not necessary. At the same time, industry and research are challenged to demonstrate sufficient awareness and consideration of people-related issues when developing and deploying new technologies and services, as well as to ensure that society continue to support innovation above stricter legislative protection.

People within the EU and US want ICT products and services that serve them and are trusted by them, and need ICT products and services for being able to deal with a number of societal challenges and individual preferences. Better EU-US ICT collaboration can hugely advance this.

PROPOSED WEBINAR AGENDA

PICASSO will organise a webinar on Privacy and Data Protection on 11 October, 15:00 UTC. Participation to the Webinar is free, and people are requested to register beforehand. Webinar registered participants will have received this draft paper in preparation of the webinar, and have been asked to read this and advance any

PICASSO has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement N° 687874.

questions coming up prior to the webinar thus allowing a further preparation of the agenda on topics that have been raised by multiple participants.

1- Welcome and purpose of the call. PICASSO, its focus, and the specific aims of this call
Maarten Botterman, Chairman of the PICASSO Policy Expert Group
2- Introduction to EU-US Privacy and data protection issues: fundamental approaches in EU and US, and developing legal frameworks.
Dr. Jonathan Cave, GNKS Consult and University of Warwick

Participatory discussion: current status and expected development in EU and US

3- Introducing the three domains 5G; Big Data; IoT/CPS.
Dr.Gerhard Fettweis, Chairman of the PICASSO 5G Networks Expert Group (tbc)
Dr.Nikos Saris, Chairman of the PICASSO Big Data Expert Group (tbc)
Dr. Sebastian Engell, Chairman of the PICASSO IoT/CPS Expert Group (tbc)
Dr. Tariq Samad, Co-Chairman of the PICASSO IoT/CPS Expert Group (tbc)

Introduction and participatory discussion:

a. Focus per domain
b. Privacy and data protection issues relevant for each domain (Taxonomy of privacy sensitivity in the domain)
c. How this affects the domain and EU-US collaboration in this domain

4- Preliminary conclusions

All introductions will be 10 minutes max followed by discussion. The total webinar will last for 90 minutes max and will be interactive. Focus is on Privacy and Data Protection aspects relevant for the PICASSO domains.

PLEASE JOIN THE PICASSO Webinar on Privacy and Data Protection on 11 October 2016, 15:00 UTC

PICASSO has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement N° 687874.