D.1.5 - [Cybersecurity Reflection Group Round Table - EU Report]

Grant Agreement number: 740647
Project acronym: AEGIS
Funding Scheme: Coordination and Support Action

Due date: 28/02/2019
Actual date: 28/02/2019
Document Author/s: [WIT, Rutgers]
Version: 1.0
Dissemination level: [PU]
Status: Final Version

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 740647

Document History			
Version	**Date**	**Comments**	**Author**
0.1	05/01/2019	Initial template	Jim Clarke
0.2	26/01/2019	Sections taking shape	Jim Clarke
0.3	12/02/2019	Sections taking shape	Jim Clarke
0.4	19/02/2019	Addition of sections by Rutgers team	Rebecca Wright, Anand Sarwate
0.5	21/02/2019	Finalising sections	Jim Clarke
0.6	25/02/2019	Final review	Dan Caprio, Jonathan Litchman
0.7	27/02/2019	Final review	Claudio Caimi
0.8	27/02/2019	Final review	Fabio Martinelli
0.9	27/02/2019	Final review	Rebecca Wright
1.0	28/02/2019	Final exec summary and conclusions, and ready for submit.	Jim Clarke

TABLE OF CONTENTS

Page

EXECUTIVE SUMMARY

On 5th December, 2018, the AEGIS project was pleased to host the "EU-US Roundtable on the Interplay of Technology & Policy in Data Privacy," a side event at the ICT 2018, which took place in Vienna on 4-6th December 2018. This major research and innovation (R&I) event attracted 4,800 visitors from all over the globe and focused on the European Union's priorities in the digital transformation of society and industry. It presented an opportunity for the people involved in this transformation to share their experience and vision of Europe in the digital age.

There were many sessions in the ICT 2018 conference, plenary, networking sessions and exhibition halls related to cybersecurity and privacy and international cooperation; therefore, it was an ideal opportunity to co-locate the AEGIS roundtable to attract participants from ICT 2018.

A significant number of policy and R&I topics of mutual benefit for cooperation between EU and US researchers in cybersecurity and privacy, including:

- As AEGIS has stressed all along with the establishment of a Reflection Group covering both Policy discussions element and Research and Innovation on the necessary technologies, there is a need to address the so-called "Privacy Paradox" of how there is a tendency to focus on the technical aspects, whereas there is a need to focus on the interplay of policy and technology instead. We need to examine the difference between how consumers and governments view privacy in an environment in which the government lags behind the private sector;
- It is very important to educate end users and industry about the potential consequences they could face if they are not taking care in relation to their data and information. GDPR is an extremely important and timely overarching framework now for data protection. We should look at ways to leverage the GDPR from the US perspective, as it is expected to take shape over the next year to avoid having a state by state approach to privacy;
- Public discussion and more research are needed to find the right balance between security and privacy;
- Data flows for a thriving economy is important, but they must be controlled; it is important for transport, energy, and daily life. Areas for future cooperation between US and EU should include: prevention, detection, response, repair (perhaps with some other steps). All of these have scope for further cooperation: research, standards, cooperation, and building capacity;
- The most common mantra being advocated is "consensus-driven and market-driven". That includes policy makers at the table, technologists, and industries that are going to be affected. From a standards point of view, we want to develop standards that are useful to individuals, industry, and policy makers;
- The topic of bridging the work of Data Privacy by Design and GDPR into a framework for having DPbD as a solution that is GDPR compliant would be an excellent cooperation activity between EU and US;
- With a move towards technologies like Artificial Intelligence (AI) and Machine Learning (ML), there is a need to look at the regional and cultural influences when designing ethical frameworks and ethical principles for these technologies in terms of what are the values and how are they evaluated;
- It was pointed out that it is not always useful to put timelines on ourselves, especially when we are in such a dynamic situation in which we cannot really predict the outcomes in the next year. What we really need to look at is how to take the learnings (regarding cybersecurity, AI, ML, distributed ledger technologies, GDPR, Privacy by Design, etc.) to see how we can be more proactive rather than reactive. The history of the Internet itself is instructive on how to best proceed together.

1 INTRODUCTION

On 5th December, 2018, the AEGIS project took the opportunity to host their "**EU-US Roundtable on the Interplay of Technology & Policy in Data Privacy**," as a side event at the ICT 2018 conference.

ICT 2018 took place in Vienna on 4-6th December, 2018. This major research and innovation event attracted 4,800 visitors from all over the globe and focused on the European Union's priorities in the digital transformation of society and industry. It presented an opportunity for the people involved in this transformation to share their experience and vision of Europe in the digital age.

ICT 2018 had four main components converging around the theme Imagine Digital – Connect Europe: Conference, Exhibition, Networking opportunities and Innovation and Start-ups forum. Since there was a number of key networking sessions accepted in areas related to cybersecurity and privacy and international cooperation during ICT 2018, the AEGIS project decided to convene their EU-US roundtable as a side-event to capitalise on the attending experts at ICT 2018. The day and time of the roundtable was carefully chosen to enable the key experts to participate to both the networking sessions of interest and the EU-US roundtable, in the co-located venues.

As information and communications technology becomes more pervasive, information and data privacy becomes of increasing importance. Used properly, data and associated analysis have the potential to significantly advance society. However, if data is used without regard to privacy of individuals or protection of the data, then individuals may be hurt intentionally or unintentionally.

If data is not permitted to be used at all due to privacy and security concerns, then the data's potential value to society is not realized. As the information that is collected about us grows in quantity, scientific and commercial value, and sensitivity, addressing these challenges is crucial to advancing innovation in areas including health, energy, and smart cities. while ensuring that privacy and associated basic rights—free speech and association, for example—are respected. Both technology and policy have key roles in protecting information and data privacy, but it is not always clear how they can best work together.

The AEGIS EU – US roundtable, with participants from both research and policy from the EU and the US, was designed to highlight progress and challenges related to enabling the use of now-ubiquitous collections of personal information while protecting the privacy of those whose data are collected. The roundtable was designed to include keynote presentations from both sides of the Atlantic, and a Panel session entitled "EU-US collaboration in data privacy and cybersecurity". US participation in the roundtable was sponsored by the National Science Foundation under grants 1636764 and 1832767.

2 OUTCOMES OF THE PRESENTATIONS SESSION

2.1 Scene setting

L-R: Yolanda Ursa, Fabio Martinelli, Rebecca Wright

The opening presenters of the roundtable explained how the main purpose of the Aegis project is for the cybersecurity and privacy communities to work together to build common ground between the US and EU on important topics related to cyber security and privacy. If we work together, we will build a framework that works for all stakeholders.

The project has carried out a comprehensive research on the landscape in the EU and US in relation to cybersecurity and privacy. Based on this analysis, a number of cybersecurity areas, ICT technologies and Applications were highlighted **for EU-US collaboration**.

The Top 5 Cybersecurity Areas identified are: Security Management and Governance; Data Security and Privacy; Education and Training; Assurance, Audit and Certification; and Network and Distributed Systems.

The Top 5 ICT Technologies identified are: Internet of Things; Cloud and Virtualization; Mobile Devices; Big Data; and Operating Systems.

The Top 5 Applications identified are: Energy; Public Safety; Transportation (including Maritime); Financial Services; and Health.

In addition, a number of recommendations on EU – US collaboration areas were identified based on a deeper analysis of what is currently happening and gatehring direct feedback from the EU and US communities on what they feel should be happening in the future. The recommendations presented and implementation suggestions for particular stakeholders given were the following:

Recommendation #1: Establish areas for collaboration that interest both the EU & the US.

Implementation Suggestions:

for Funding programme managers: Develop specific programs within the usual CSP R&I funding programs (or cross-programme collaborative projects) on areas of mutual interest.

Recommendation #2: Take an international approach to cybersecurity.

Implementation Suggestions:

for Government: Increase efforts to counter cross-border cybercrime.

for Funding programme managers: Establish cross-programme calls for R&I projects on countering international cybercrime.

Recommendation #3: Invest in international cybersecurity projects.

Implementation Suggestions:

for Government: Increase funding for cybersecurity.

for Funding programme managers: Redirect or allocate money for international CSP R&I projects.

Recommendation #4: Establish or improve international coordination between funding programs.

Implementation Suggestions:

for Funding programme managers: Find and establish contacts with cross-Atlantic funding agencies. Organise collaborative programmes. Specify common goals, funding procedures and rules for collaboration.

Recommendation #5: Reduce legislative barriers for cybersecurity and privacy collaboration.

Implementation Suggestions:

for Policy makers: Harmonize legislation requirement frameworks. Develop special cases for the research use of data to reduce unnecessary burdens.

for Funding programme managers: Cooperate with other research funding programmes from other countries to establish basic rules for legal issues in international projects.

Recommendation #6: Promote cybersecurity information sharing.

Implementation Suggestions:

for Government: Encourage information sharing between governmental agencies at national and international levels. Provide researchers access to this data.

for Funding programme managers: Support research of information sharing schemas, especially ones guaranteeing security and privacy.

Recommendation #7: Invest in cybersecurity education and training.

Implementation Suggestions:

for Government: Create special collaboration programmes for cyber education and training similar to the Marie Curie Actions for the exchange of PhD students.

for Funding programmes managers: Devote more attention to projects that provide innovative methods for cybersecurity education and awareness raising. Support international cybersecurity training and awareness event participation.

Recommendation #8: Support securing Critical Infrastructure.

Implementation Suggestions:

for Funding programmes managers: Establish programmes for collaborative projects in specified fields (Energy, Water, Nuclear, etc.) and encourage the information sharing in these domains.

The opening speakers welcomed the feedback from the audience during the round table today, and/ or following the event. The full set of presentations can be found at: https://drive.google.com/drive/u/1/folders/1K_KyWNicSukgUcpySmSPSFmfCLvm52CC

2.2 Main take-aways from the Presentation session

The speakers focussed on a number of areas of potential collaboration between EU – US cybersecurity and privacy researchers. These areas are summarised here.

Ken Calvert, NSF

The National Science Foundation (NSF) produced a personalized video greeting for the AEGIS EU-US roundtable with the key message that through its Secure and Trustworthy Cyberspace program, the NSF takes a comprehensive, interdisciplinary approach to cybersecurity and privacy. In the video, it was stressed that a critical first step for collaboration is a demonstration of interest and collaborative research potential and a project like AEGIS is well positioned to foster both of these requirements. It was also highlighted that international cooperation can provide a solution to many compelling issues that we need to be addressed together across the Atlantic.

Aljosa Pasic, Atos

An insightful presentation was made on GDPR and data usage control, clearly differentiating between data access on the one hand and data usage control on the other. The presentation focussed on the challenges related to dealing with real-time data, where it's not just only about content management, as there are other issues here related to GDPR. Having access control is not enough, and the parties are bound to comply with obligations at two levels: 1. Contractual terms and conditions specifically set forth and agreed upon by the parties; and 2. Mandatory rules arising from the applicable law(s), for example GDPR Article 7, conditions of consent or transfer of personal data within the EU/EEA. In term of data usage control policies, "transfer" refers to the moving of data, but also when an employee outside the EU views data. Moreover, any access to data outside of EU/EEA counts as a transfer, which leads to a number of challenges, including tracking data flows oustide EU/EEA, distributed enforcing, adaptability of remote systems and services, and legal and other guarantees outside EU/EEA. A number of interesting projects working in this area were presented including CoCoCloud, PAPAYA[1] – Platform for Privacy preserving data analytics, and AutoMat[2] Vehicle Big Data Sharing Platform.

[1] https://www.papaya-project.eu/
[2] http://www.automat-project.eu/

Alexandra Wood, Harvard University

A presentation was made on the Hybrid Legal Technical Concepts of Privacy, where it was stressed that what we have learned is that privacy often relies on concepts that have both a technical and legal meaning. The motivational factors highlighted included the inadequacy of the current regulatory framework for privacy, where the law is ill-suited to provide comprehensive protection in the digital age. There is a reliance on concepts such as PII, endorsement of ad hoc approaches that fail to provide adequate protection (e.g., HIPAA Privacy Rule safe harbor method), and recognition of a limited set of privacy failures (e.g., record linkage). The underlying privacy concepts seem fundamentally unable to keep up with the pace of technological change and they require frequent amendment. Moreover, the law's requirements are ambiguous, making it difficult, if not impossible, to understand what they are designed to protect. Other motivations explained in detailed included the weaknesses of commonly used privacy concepts, and the emergence of new privacy concepts. Some examples of these include Contextual integrity introduced by Nissenbaum in 2004 and Differential privacy introduced by Dwork, McSherry, Nissim, and Smith in 2006. The work related to Hybrid concepts was described in which the privacy concepts are neither purely legal nor purely technical; they have an inherent "hybrid" legal-technical nature. With these concepts, adopting an understanding of privacy that is consistent across its technical and normative dimensions will be critical to ensuring personal data are adequately safeguarded over the long term. Conceptual gaps between existing technical and normative concepts create challenges for arriving at a universal notion of privacy. Understanding the hybrid nature of these concepts and developing tools for implementing them is necessary to bridge the gaps between the current legal and technical understanding of privacy. In relation to Hybrid concepts, considerations for future regulations were given, including that the regulations should articulate clear goals for privacy protections and these goals should be line with the scientific understanding of privacy and regulations should move away from implicitly or explicitly endorsing ad hoc de-identification techniques. An example of this would be the guidance on European data protection law outlines goals that go beyond the traditional notion of de-identification, providing protection against singling out, linking, or inferring an individual's personal data from a dataset. These concepts have not yet been defined precisely and formally from a mathematical perspective, but they aim to describe a goal and it would be an excellent topic for EU-US collaboration.

Peter Fatelnig, Minister-Counsellor for Digital Economy Policy, Delegation of the European Union to the United States

The perspective from the EU Delegation in the US was given to the roundtable as to the importance of collaboration between EU and US on cybersecurity and privacy. It was pointed out that the EU's leadership in regulatory and data privacy protection due to their GDPR is well recognised in the US and further afield; interestingly, the conversation about privacy and data protection has evolved a significant amount in the US over the past 12 months. For example, California has enacted its own regulation, the Consumer Data Privacy Act, which will enter into force in Jan. 2020. It is well recognised that the EU has been moving very fast with GDPR and it has been using it as an instrument not only in the EU but also with other countries, as we are witnessing a broadening of the GDPR conversation around the world. It is possible that there could be action US on a federal privacy law as early as 2019, as it is recognised that having different state-based privacy laws wouldn't be the best way to proceed.

Tomas Sander, Intertrust

The use of Privacy by Design (PbD) in the era of the GDPR was the topic of the next presentation. Privacy best practices have been done before but when it comes to GDPR, there isn't a solution that will always work as yet. There are a number of challenges that the international communities can address together to address the situation, including no commonly agreed PbD methodology, it is unclear what organizations need to implement under GDPR to "do" Data Protection by Design (DpbD), existing PbD frameworks don't necessarily lead to broad GDPR compliance, or may not be a direct or cost-effective way, and limited resources for (i) PbD process implementation and (ii) follow through on findings. As a result, most companies don't have a comprehensive PbD program as of yet. When you go to engineers and tell them that you want them to implement GDPR and privacy requirements, you have to have a good reason to convince them to implement these measures. They are not going to do it just for fun. Therefore, the EU and US communities should work together to identify what an organization with limited resources can do to start PbD process and how can we create better incentives for adoption. As a first step, it was recommended that we create a simple methodology (templates and support material, policies, guidelines) for PbD process that supports broad adoption in order to allow organizations to move quickly from state of ad-hoc privacy reviews to a systematic, documented, repeatable PbD process, even if not perfect. A DPbD process was outlined that

would ensure accountability for DPbD, which would include the inclusion of required DPbD documentation consisting of completed evaluation form and a document that tracks privacy requirements or mitigations. Also part of the process is to respond to customer requests about your DPbD practices with DPbD templates and process, but no review details, and applying vendor due diligence about PbD creates incentives for adoption through inclusion of PbD in due diligence questionnaires. Additional DPbD support could be assured with the development of specialized questionnaires for technologies with AI and Machine Learning, Blockchain etc. and the creation of DPbD policy templates with ways to strengthen impact in organizations. Future work for EU-US collaborators in this subject would be a working on a simple DPbD process that helps organizations meet substantive GDPR requirements for products and processes. Items to tackle together would include refine methodology, add supporting resources, and clarify incentives.

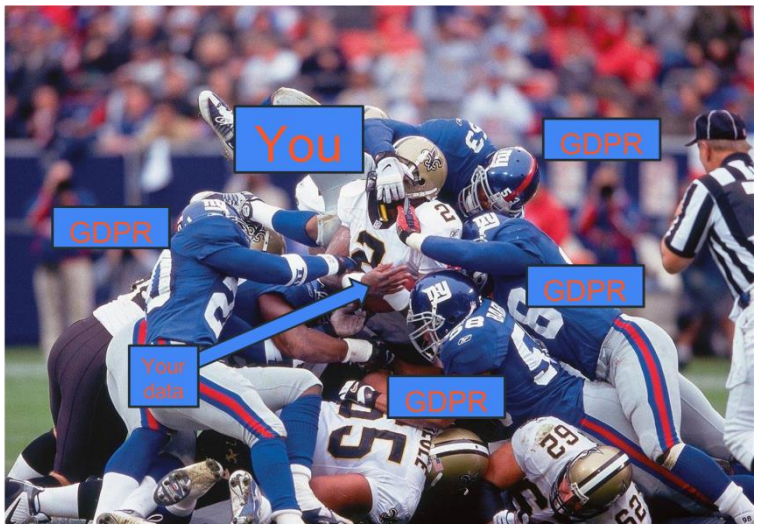
Evangelos Markatos, FORTH

The next presentation was a deeper dive into the legal aspects of GDPR. GDPR is a regulation (a European "Law") to harmonize data privacy laws across Europe, protect and empower all EU citizens' data privacy, and reshape the way organizations across the region approach data privacy. To collect data you need a legal basis (do you have the right to collect/process data?. For example, Explicit Consent (Article 6 – normal data), National Law (Article 9 – special data), and there are exceptions for Research (Article 9), where is says …processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. However, it was pointed out that Member States may introduce further conditions for health data (Article 9 (4)), where it says ...Member States may maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health. There are a number of rights for citizens, including: Right to Information (art. 13 and 14), Right to access to the data (article 15), Right to object (to the processing of the data) (article 21), Right to erasure (article 17), Right to be forgotten, Right to not be subject to Automated Decision Making (article 22), Right to Portability (article 20), Transfer your data to another controller, and Right to Notification of Personal Data Breach (article 33). Additional safeguards for processing of data were presented in detail, including anonymization, pseudonymization, data minimisation, and encryption. Ominously, some examples of breaking these safeguard techniques were given.

Aloni Cohen, Massachusetts Institute of Technology

The next presentation started out with the question and answer, "Is singling out still a risk? Yes, because if you pseudonymize someone, you can still single them out. The intuitive meaning of ´singling out´ means that there is exactly one person that has these attributes." This causes a problematic conceptual divide whereas law requires legal guarantees, but crypto offers mathematical guarantees. However, law is typically imprecise and subject to interpretation and disagreement. How do we bridge the gap? Goals are to 1. Understand singling out and its relationship with cryptographic notions of privacy, and 2. Provide a necessary condition for data anonymization. An approach to take is 1. Extract relevant text, 2. Define singling out, mathematically, and 3. Analyze as a stand-alone notion and with respect to cryptographic notions. Differential privacy was defined as privacy whereby the output "doesn't depend" on any single persons data. As to whether it is secure against singling out, it is probably according to the modelling. As to whether it provides adequate "anonymization" under the GDPR, it isn't clear as preventing singling out attacks is necessary, but probably not sufficient. Therefore, more research is needed here.

As shown on the right, an interesting analysis of a person's (represented as the quarterback with the football) and their data being represented as the football they are carrying, throwing, or kicking, whereas GDPR is attempting to protect the data from the other players, was given during the presentation.



Following on from this analogy, every time you bump into a player, or want to throw the ball, or kick a field goal, where GDPR is required to protect the information and data as represented by the football, there is an additional cost involved not necessarily sought by the user; Consequently, these costs matter in a tight business environment, so there are implications of increased cost of GDPR compliance, highlighting the tensions between cybersecurity and privacy that can exist. They are not always aligned. It was reiterated that public discussion is needed for where is the right balance.

3 OUTCOMES OF THE PANEL SESSION

3.1 Scene setting

L-R: Jim Clarke (missing from photo), Maria Palombini, Felix Barrio, Claudio Caimi, Camille Sailer, Miguel Gonzalez-Sancho, Pedro Pavon, Jonathan Litchman

The main objective of the Panel session was to exchange views on the interplay between privacy and cybersecurity technologies, and build synergies and solve problems experienced on both sides of the Atlantic. The Panellists were asked in advance to outline from their perspectives how Privacy is being addressed in the US and EU, respectively, and what concrete steps we can take moving forward together.

Each panellist was given an opportunity to introduce themselves, their organization and role, and set the scene about their perspectives in privacy and cybersecurity. The panellists were asked to cover the following items in their opening statements:

1. What are the common problems that we need to address together on enhancing privacy and cybersecurity, and where are areas that complement each other with EU-US collaboration?
2. What barriers do you see to EU-US collaboration in data privacy and cybersecurity?
3. What should EU-US collaboration on privacy and security look like in 5 years?
4. More concretely, what are the next implementation short-term tactical and longer-term strategic steps) to deal with research and innovation challenges of privacy and cybersecurity?
5. What are successful examples of EU-US collaboration in data privacy and cybersecurity?

3.2 Main take-aways from the Panel Session

L-R: Jim Clarke, Maria Palombini, Felix Barrio, Claudio Caimi

A number of areas for mutually beneficial EU-US cooperation in cybersecurity and privacy were illuminated during the panel session. These are summarised here.

An area of cooperation could be the so-called ”Privacy Paradox” of how there is a tendency to focus on the technical aspects, whereas there is a need to focus on the interplay of policy and technology, as entitled for this roundtable. We need to examine the difference between how consumers and governments view privacy in an environment where government lags behind the private sector. Consumers are already concerned; government is only starting to catch up. We are living in an evolving situation moving from Data -> Big Data -> Artificial Intelligence -> to other significant advances such as smart cities and autonomous vehicles. We are also living in a world that is focused on the monetization of data, where users’ data is regularly being sold and used without the general knowledge of the consumers. The other paradoxical part of the story was raised that a segment of the end users, whether knowingly or unknowingly about their privacy situation, will still use anything on the Internet, and they haven’t been clamouring for government protection. Therefore, to address this, it is very important to educate end users and industry about the potential consequences they could face. GDPR is extremely important and timely overarching framework now for data protection. We have a new European digital marketplace, and privacy is critical not only for consumer security and privacy protection but also for the development and support of a robust and safe marketplace.

Balance between security and privacy was another area raised by the panel. Following the football analogy in the presentation by Aloni Cohen, every time you bump into a football player representing GDPR, there is an additional cost involved. And every field goal is a cost of the touchdown not being sought. These costs really do matter in a tight business environment, so there are implications of the increased cost of compliance resulting in a significant tension between cybersecurity and privacy coming into play. For example, the way information and system access of employees within companies is similar to a surveillance state that ignores privacy rights of the employees. Likewise, this can be seen by consumers in an environment where security trumps privacy. Therefore, public discussion and more research are needed to find the right balance between security and privacy.

Cybersecurity is a foundational requirement for digitalization, the same way safety is for transportation. A number of values are protected by having strong cybersecurity, and privacy is one of them (though despite the tension noted

previously). Data flows for a thriving economy is important, but they must be controlled; it is important for transport, energy, and daily life. Areas for future cooperation between US and EU should include: prevention, detection, response, repair (perhaps with some other steps). All of these have scope for further cooperation: research, standards, cooperation, and building capacity.

The most common mantra being advocated is "consensus-driven and market-driven". That includes policy makers at the table, technologists, and industries that are going to be affected. If policy drives the conversation alone, people feel that policy is imposing on industry, and on citizens. The question of cybersecurity and privacy: they go hand-in-hand and people use them interchangeably. We look at the empowerment of the individual citizens, but not to disintermediate or punish. In healthcare, for example, the power of "protect" has had limitations and there are philosophical questions. From a standards point of view, we want to develop standards that are useful to individuals, industry, and policy makers.

The topic of bridging the work of Privacy by Design and GDPR that was presented earlier could also feature as a good topic for EU-US cooperation. In the EU, there has been earlier work on PbD carried out in the EU PRIPARE (PReparing Industry to Privacy-by-design by supporting its Application in REsearch project)[3], which was funded by the same unit as AEGIS a number of years ago, which contributed to the ISO/NP 23485 Consumer protection – Privacy by design for consumer goods and servers. Taking this forward into a framework for having DPbD as a solution that is GDPR compliant would be an excellent cooperation activity between EU and US. A number of the AEGIS partners and speakers today were actively involved in the PRIPARE project.

Topics like Artificial Intelligence (AI) and Machine Learning (ML) have really changed the conversation about passive data and what is being done with all the collected data. The concerns about responsible use have increased drastically and this must be addressed e.g. Cambridge Analytica problem. There is also the complexity of the regional / cultural factors involved in how the end user feels. An example was given about a self-driving car having to decide whether to kill a grandmother or a baby, and the regional/cultural nature of the responses would be quite different, which highlights the need for ethical frameworks and ethical principles for these technologies in terms of what are the values and how are they evaluated. Regarding cybersecurity, it was cautioned that we should be careful not to focus on data protection as a mechanism for reigning in AI. An example of the Model-T was used to highlight the situation. At the time of the Model-T, the leader of the patent office thought they would soon not need a patent office because all the inventions had been invented. In addition, there were safety concerns that cars were less safe than the horse and buggies they replaced, even though those were not themselves completely safe.

In the EU, GDPR was designed in 2016 and came into being in May, 2018. It is clear that it is now being discussed quite a lot in the US. A question was asked whether it is just because everyone got annoying emails following the onset of GDPR, or can we predict when something will come into relevance in the US in terms of GDPR? It was felt by the panel that perhaps the topic has been coloured a bit more by the media recently picking up on GDPR. However, it was pointed out that US industry has been discussing it for quite some time (e.g., Google's plan to put 600 engineers on it in 2017 or thereabouts). Clearly, the cost of non-compliance and messaging that it would apply to non-EU companies doing business in the EU and some examples were cited of some of these taking place already.

[3] http://pripareproject.eu/

The panel was questioned about standardization in relation to privacy and ethics. Unlike in standardisation in chip design, where it's somewhat easier because there are a small number of manufacturers who need to be involved, for privacy and ethics, the situation is quite different, as everyone involved has some interaction with it. Who are the relevant stakeholders and how do you handle standardization in privacy and ethics. The panel's response included how compatibility is a goal of standardization, but can be hard due to the large number of companies affected. Thus, they could aim at least for portability. Some areas of standardization in mobility and spectrum have been controversial, but still there are also fewer stakeholders. It is necessary to bring the multi-stakeholders to the table with the technologists when involved in creating technical standards and operationalizing technical controls. In any case, it is not an easy question to answer because how do you standardize good behaviour? It was pointed out that GDPR has both ex-post and ex-ante aspects such as behaviour, data for research purposes; when do you have to re-ask for consent? Also, there may be different answers across different sectors. You can't always regulate to the detailed level; the regulation is broad and based on principles. Some cases are not straightforward, more work is definitely needed.

A final question was put to the Panel: Imagine us being here next year talking about the same issues (why is GDPR so important) and also value of data that we didn't talk about (evolution of business models, who owns the data, what's the customer's share). How far do we expect regulation to keep up and keep going? How does it relate to business models and the need to be agile? I don't believe regulation is the only solution, maybe there should be some market evaluation and dynamics. What do each of you think the future brings, particularly around data monetization? The panel members responded that consumers are becoming aware of data monetization as an issue, and even though there might be a small majority who don't seem to care, there is growing anger against the technology behemoths. Therefore, pressure will need to be placed on legislators to create sensible legislation in relation to this important issue (even though that is a slow process). There are even creative companies that are busy creating models to move forward with a business model that attracts those angry customers away from the current behemoths. Some of this type of activity is being discussed in the EU's Next Generation Internet (NGI) initiative, which is looking at the reimagining of the Internet in ten or more years' time of a more human-centric internet that respects privacy and human values as a core foundation. It was felt that monetization of data must be addressed more aggressively. While data can be given for some known advantages (e.g., using Google maps, ad-based services, etc.), the end user needs to know how their data is being used. To address this, regulation is essential. Governments represent the people, while companies defend their own interest and the interests of their investors. Regulation is key to address this and drive desirable behaviour, promote societal values, etc. Of course, there are different opinions on desirable societal values. Taxation is a useful example to consider (tax for what purposes). There is a need for more capabilities to promote privacy and therefore, the next year is a year for lessons learned, especially how to reinforce SMEs. It was pointed out that it is not always useful to put timelines on ourselves, especially when we are in such a dynamic situation in which we cannot really predict the outcomes in the next year. What we really need to look at is how to take the learnings (regarding cybersecurity, AI, ML, distributed ledger technologies, GDPR, Privacy by Design, etc.) to see how we can be more proactive rather than reactive. The history of the Internet itself is instructive on how to best proceed together.

4 CONCLUSIONS AND NEXT STEPS

The mix of presentations and panel discussions at the Cybersecurity Reflection Group Round Table – EU held in Vienna, Austria, highlighted a significant number of policy related and research and innovation topics of mutual benefit for cooperation between EU and US stakeholders in cybersecurity and privacy.

The audience was requested to reflect on the applications and recommendations of the AEGIS project. As these were considered and no particular counter-recommendations were made during or after the meeting, the project recommends the European Commission to consider these for future funding.

The **Application areas** highlighted for **EU-US collaboration are the following:**

The Top 5 Cybersecurity Areas identified are: Security Management and Governance; Data Security and Privacy; Education and Training; Assurance, Audit and Certification; and Network and Distributed Systems.

The Top 5 ICT Technologies identified are: Internet of Things; Cloud and Virtualization; Mobile Devices; Big Data; and Operating Systems.

The Top 5 Applications identified are: Energy; Public Safety; Transportation (including Maritime); Financial Services; and Health.

The **Recommendations and implementation Suggestions** for particular stakeholders given are the following:

Recommendation #1: Establish areas for collaboration that interest both the EU & the US.

Implementation Suggestions:

for Funding programme managers: Develop specific programs within the usual CSP R&I funding programs (or cross-programme collaborative projects) on areas of mutual interest.

Recommendation #2: Take an international approach to cybersecurity.

Implementation Suggestions:

for Government: Increase efforts to counter cross-border cybercrime.

for Funding programme managers: Establish cross-programme calls for R&I projects on countering international cybercrime.

Recommendation #3: Invest in international cybersecurity projects.

Implementation Suggestions:

for Government: Increase funding for cybersecurity.

for Funding programme managers: Redirect or allocate money for international CSP R&I projects.

Recommendation #4: Establish or improve international coordination between funding programs.

Implementation Suggestions:

for Funding programme managers: Find and establish contacts with cross-Atlantic funding agencies. Organise collaborative programmes. Specify common goals, funding procedures and rules for collaboration.

Recommendation #5: Reduce legislative barriers for cybersecurity and privacy collaboration.

Implementation Suggestions:

for Policy makers: Harmonize legislation requirement frameworks. Develop special cases for the research use of data to reduce unnecessary burdens.

for Funding programme managers: Cooperate with other research funding programmes from other countries to establish basic rules for legal issues in international projects.

Recommendation #6: Promote cybersecurity information sharing.

Implementation Suggestions:

for Government: Encourage information sharing between governmental agencies at national and international levels. Provide researchers access to this data.

for Funding programme managers: Support research of information sharing schemas, especially ones guaranteeing security and privacy.

Recommendation #7: Invest in cybersecurity education and training.

Implementation Suggestions:

for Government: Create special collaboration programmes for cyber education and training similar to the Marie Curie Actions for the exchange of PhD students.

for Funding programmes managers: Devote more attention to projects that provide innovative methods for cybersecurity education and awareness raising. Support international cybersecurity training and awareness event participation.

Recommendation #8: Support securing Critical Infrastructure.

Implementation Suggestions:

for Funding programmes managers: Establish programmes for collaborative projects in specified fields (Energy, Water, Nuclear, etc.) and encourage the information sharing in these domains.

The distinguised panel session has highlighted a significant number of topics that should be included in the above recommendations, including the following:

- The need for another project to follow the integrated approach of AEGIS, which is including a **frequent policy discussion element and research and innovation element** when dealing with the interplay between cybersecurity and privacy across the Atlantic;
- **Education of end users and industry** about the potential consequences in relation to their data and information, especially in the era as we move into technologies like Artificial Intelligence and Internet of Things;
- We should look at ways to **leverage the GDPR from the US perspective**, as it is expected to take shape over the next year to avoid having a state by state approach to privacy;
- Public discussion and more research are needed to find the right balance between security and privacy;
- Areas for future cooperation between US and EU should include: control of data flows, prevention, detection, response, repair (perhaps with some other steps). All of these have scope for further cooperation: **regular policy discussions, research, standards, international cooperation, and building capacity;**
- The topic of **bridging the work of Data Privacy by Design (DPbD) and GDPR** into a framework for having DPbD as a solution that is GDPR compliant would be an excellent cooperation activity between EU and US. There has already been some work in this area and there should be funding to continue it;
- With a move towards technologies like Artificial Intelligence (AI) and Machine Learning (ML), there is a need to **look at the regional and cultural influences when designing ethical frameworks and ethical principle**s for these technologies in terms of what are the values and how are they evaluated;
- There is a need to be **more proactive than reactive in our research and innovation** in the dynamic digital world we are living. Working together on cybersecurity and privacy is a multi-stakeholder activity that requires us to learn from our experiences, especially in relation to new technologies like AI, ledger technologies, privacy by design and GDPR.

APPENDIX 1. FINAL AGENDA

The agenda of the "EU-US Roundtable on the Interplay of Technology & Policy in Data Privacy was the following:

16:00-16:15: Welcome and overview, Yolanda Ursa, AEGIS Coordinator, Fabio Martinelli, CNR, and Rebecca Wright, Rutgers University

16:15-16:30: "GDPR and data usage control," Aljosa Pasic, Business Development Director, ATOS

16:30-16:50: "Hybrid Legal-Technical Concepts of Privacy," Alexandra Wood, Harvard University, Berkman Klein Center for Internet & Society

16:50-17:00: "EU-US Digital Cooperation, cybersecurity and privacy," Peter Fatelnig, Minister-Counsellor for Digital Economy Policy, Delegation of the European Union to the United States

17:00-17:20: "Going mainstream: Privacy by Design," Tomas Sander, Intertrust

17:20-17:40: Break

17:40-17:55: "GDPR and Internet Security for Research," Evangelos Markatos, Head of the Distributed Computing Systems Laboratory, FORTH-ICS

17:55-18:15: Aloni Cohen, Massachusetts Institute of Technology

18:15-19:00: Panel: "EU-US collaboration in data privacy and cybersecurity"

Chairs: Jim Clarke, WIT and Jonathan Litchman, The Providence Group

Panelists:

- Miguel Gonzalez-Sancho, Head of Cybersecurity Technology and Capacity Building Unit, DG CONNECT, European Commission

- Camille Sailer, President and CEO, European American Chamber of Commerce New Jersey

- Felix Barrio, Head Manager of Content and Research on Cybersecurity, Spanish National Cybersecurity Institute- INCIBE

- Maria Palombini, Director, Communities and Initiatives Development, Emerging Technology, GBSI, IEEE Standards Association

- Pedro Pavon, Global Managing Counsel on Data Protection, Oracle

- Claudio Caimi, Program Manager IT Security, HPE

19:00-20:00: Cocktail reception