PRIVACY AND CYBER SECURITY ON THE BOOKS AND ON THE GROUND

Ingolf Pernice, Jörg Pohle (Eds.)

ALEXANDER VON HUMBOLDT INSTITUTE FOR INTERNET AND SOCIETY
BERLIN, GERMANY

The Alexander von Humboldt Institute for Internet and Society (HIIG) explores the dynamic relationship between the Internet and society, including the increasing penetration of digital infrastructures into various domains of everyday life. Its goal is to understand the interplay of social-cultural, legal, economic, and technical norms in the process of digitisation.

Alexander von Humboldt
INSTITUTE FOR INTERNET
AND SOCIETY

FOREWORD

This first conference in a transatlantic dialogue on privacy and cyber security, held in November 2017 at HIIG in Berlin, brought together an eminent transdisciplinary group of experts from academia, administration, business and civil society from both sides of the Atlantic. It was carried by the hope to find a deeper understanding of the issues at stake and common approaches allowing the internet and digitalisation in general, to develop in the interest of all, across the Atlantic and perhaps worldwide. A "Transatlantic Technology and Security Working Group" might emerge from this conference and from a second conference planned for 2018 in New York. We aim to providing for a forum offering a discursive room for a lasting open, fact-based and creative dialogue on key questions of our society.

The evolving digital society is global, and with it we are facing global challenges requiring global solutions. While the questions we are discussing are extremely complex, I believe that with a certain degree of simplification it is possible to talk about a "magic square" —pointing to tensions and synergies among four aims and issues:

Free flow of data as a precondition for free trade of goods and services worldwide, the functioning of the global financial markets, communication and information, education and participation.

Data protection and security as a basic precondition for the exercise of our common fundamental rights, condition of citizens' trust and participation in markets and politics, fundament of open, free and undistorted democratic processes.

Law enforcement and surveillance as a necessity for national and international security, requirement of the rule of law, but also subject to it, condition for functioning democratic processes in a digital society.

Intelligence services and operations providing governments information about each others activities, allowing to discover and determine security risks, and building trust, assisting governments in the difficult task of attribution of cyber threats.

Two key questions already laid out in the outline to this conference were to be discussed in our panels. What is the impact of European Data Protection Regulation on the ability of global companies to provide for cyber security? And what are the most effective frameworks in the EU, the US and globally providing for and governing cyber security? We will have to discuss whether GDPR is, perhaps, a threat to cybersecurity —if authorities

have no access to data at any relevant place, how can they protect cybersecurity?— or if it is a necessary tool of and condition for effective data protection? How safe and private are data if their storage or processing is subject to cyber-attacks? And what about situations, like in the Microsoft case, when law enforcement authorities compel globally acting companies to give access to data stored in a country where any transfer of data to other countries and their authorities is prohibited? Exposing a company to such conflicting legal duties as such could be a flagrant breach of the rule of law. It would be the opposite of "law" enforcement.

What are the global companies' responsibilities for active cyberdefence. Do they have a right —or duty?— to resist governments requests for providing technologies for data breaches and cyber attacks? Who is responsible for cyber security and effective data protection? Five scenarios have been laid out in the outline to this conference. There are good reasons to believe that governments, industries and businesses as well as the individual users are responsible all together, that there is a common responsibility. We should consider (global) cybersecurity as a matter of governance instead of adopting a top down approach based upon regulation —who should be the regulator? Who is it to enforce any such regulation?

The same applies to data protection: global challenges need global solutions. In a longer perspective, thus, we would need to establish principles and structures for effective cybersecurity and global privacy governance, in order to securing a smooth functioning of the internet. Step one could be an intensive transatlantic dialogue and cooperation, as we are trying to promote with our conferences. But the dialogue should, of course, reach beyond this in order to build up a discourse on globally applicable solutions. We believe that this conversation must include industry, public administration and governments, civil society and academia. The outcome of this first conference, as presented hereafter, confirms that this inclusiveness allows better understanding and creative solutions, and it encourages us to pursue the idea and invite all those interested to participate actively in the discourse.

Ingolf Pernice

CONTENTS

U.S. AND EUROPEAN CYBER SECURITY AND PRIVACY POLITICS AND STRATEGIES: THE CHALLENGES AHEAD

RESPONSIBILITIES, RIGHTS AND ENFORCEMENT

LOOKING FOR COMMON GROUND IN A GLOBAL PERSPECTIVE

THE REGULATORS' TOOL BOX

Privacy and Cyber Security on the Books and on the Ground: An Introduction

MARIE-CHRISTINE DÄHN, INGOLF PERNICE & JÖRG POHLE

On 6 and 7 November 2017, the Alexander von Humboldt Institute for Internet and Society (HIIG) invited researchers and practitioners to a transatlantic conference entitled "Privacy and Cyber Security on the Books and on the Ground" in Berlin, Germany. The conference was organised in collaboration with New York University (NYU) as the first of two conferences. The second will be held in New York in the autumn of 2018. The aim is to address the tense transatlantic relationship in cyber law and politics with special regard to the relationship between cyber security and data protection. The previously distinct areas of technology, law and policy have begun to merge and the legal and policy frameworks of privacy and data protection, surveillance, and cyber security have successively converged. Thus, in this context, the first conference brought together experts from many varied backgrounds, including the fields of cyber security, data protection, law and governance, but also representatives from security agencies, businesses and the sphere of politics in order to shed light on the (global) implications of the EU's General Data Protection Regulation (GDPR) for companies with regard to cyber security requirements, and possible effective frameworks for regulating and governing cyber security. In the course of the discussions, current problems in the field were analysed, concepts differentiated and compared, and approaches for solutions discussed. This process succeeded in drawing together the often relatively independent discourses taking place in the USA and Europe.

TRANSATLANTIC IMPACT OF EU DATA PROTECTION LEGISLATION

The EU's new General Data Protection Regulation ushers in a new era of data protection law in the EU. With both global scope and prescriptive force, the GDPR seeks to institutionalise and globalise a view of privacy and data protection that revolves around the protection of data subjects' fundamental rights and freedoms in the collection and use of personal data for commercial purposes. This European approach has long been criticised (whether rightly or not) as de-emphasising other important social values, including economic liberty, freedom of speech, and national security. It is also widely believed that the implementation of the GDPR in May 2018 will result in reduced flows of data from Europe to the U.S. and elsewhere, a view that has been reinforced by the results of recent litigation in the EU, in particular the Schrems case and others, and ECJ opinion 1/15 on the PNR agreement with Canada.

Critics also consider the implementation of the GDPR to be a threat to cyber security. State-of-the-art cyber security protection often relies on the collection and analysis of large

—and ever-increasing— amounts of data. Companies must know what is happening on their networks in order to determine when anomalous behaviour is taking place, for example, and they are being increasingly asked to share that data with other companies and with governments in order to enhance collective defences against cyber threats. Indeed, in some circumstances, cyber security regulations in the U.S. require companies to take certain measures that may be prohibited (or at least are cast into doubt) by the GDPR, creating the potential for a conflict of laws.

There is a significant question, therefore, about the impact of the GDPR on the ability of global companies to engage in effective cyber defence. Privacy and effective data protection, on the other hand, require the security of personal data and processing, so that cyber security plays a role also in GDPR. Determining what any such impact might be depends on an understanding of cutting-edge technical and policy requirements for cyber defence in moderately-sized to large companies; a detailed understanding of the GDPR and associated requirements; and a fine-tuned understanding of U.S., European and global regulatory requirements.

GOVERNANCE FRAMEWORKS

At the same time, significant questions have emerged about the best practices for developing a regulatory architecture for cyber security, as the U.S. and its European allies are just beginning to develop a governance framework for cyber security challenges. Any such regulatory architecture must answer questions about the respective roles of public and private sectors in cyber security; the cyber security obligations of private companies; what companies must do when confronted with conflicting obligations; how information about threats and responses flows among the various actors in the system; and who is to be held responsible in the event of an incident; among many other things.

As there is increasing awareness of cyber threats, a range of different frameworks is available for governing the response to the threat. Different countries have pursued different approaches (and sometimes embrace different frameworks simultaneously), but the broad options include:

- Primary government responsibility for monitoring and providing protection against cyber threats;
- Active government involvement in threat detection but primary private sector responsibility;
- Detailed and prescriptive government regulation of private sector obligations, but primary private sector responsibility for addressing the threats;
- Vague government regulation of private sector obligations, with primary private sector responsibility for addressing the threats;
- Empowerment of intermediaries (e.g. ISPs) to monitor for threats and engage in responsive activity.

As threats have become more acute in the last few years, governments have embraced all of these approaches at different times but the problem is that there is still no consensus on which approach is best, or, more accurately, which approach can achieve which security objectives and at what cost to other values. The conferences seek to provide greater clarity to regulators and regulated alike about the trade-offs involved in the different approaches to governing complicated questions of technology and security.

RESULTS OF THE FIRST CONFERENCE AND THE ROAD AHEAD

As an overall result, the conference's participants came to the conclusion that, despite the different foundations of, and approaches to, privacy and data protection in the EU and the U.S., various similarities can be drawn. Moreover, there are opportunities to further the development of the transatlantic cooperation in this area. The attendees pointed in particular to the potential of mutual learning between U.S. and EU actors in the sphere of privacy and data protection as well as cyber security. This seems to be particularly important with a view to ensuring the free flow of data across the Atlantic in times when not only transatlantic agreements like on PNR, SWIFT, or the Privacy Shield are threatened because they may not meet the requirements established by the ECJ, but even fundamental concepts of terms remain to be clarified such as the notions of equivalent protection or what harm to data subjects the GDPR is to protect against.

As far as privacy and data protection is concerned, the new data protection framework of the EU, the General Data Protection Regulation, has been the frequent focus of discussions. While mainly applicable to the European Union, the GDPR also has important implications for the U.S. and the world at large. In general, it has been remarked that the harmonisation of the legal framework entails many improvements —for example, the empowerment of DPAs or the enhancement of instruments such as binding corporate rules— but still leaves many questions unanswered. Rules often leave much room for interpretation and particularly from a practical economic perspective it is not always clear how to comply with them. Besides, the balance between the rights of individuals and companies' demands has also been raised as an issue, one that needs to be discussed more deeply in the field of privacy and data protection generally. Another aspect that has sparked lively debate is the enforcement of the GDPR and its shortcomings. The regulation, for instance, does not take into account the different sizes of companies while imposing the same sanctions on them for violating the GDPR's provisions. Another point that calls for further debate is the legal interpretations of the GDPR and the initial experiences of its application after its entry into force on 25 May 2018. What has become apparent, however, is the necessity to combine approaches in specific areas of privacy, data protection and cyber security —more specifically, in Art. 25 GDPR, which regulates both security by design and data protection by design. Some of the best practices have been outlined by Rubinstein (see relevant paper) and computer scientists introduce security engineering in this regard, but the exact method of implementation remains debatable.

Overall, in this first conference there was wide agreement that fragmented legal frameworks, notably in the area of privacy and data protection, should be harmonised in order to become fully effective, and the GDPR has been mentioned in this respect as a possible blueprint.

The discussants, moreover, focused on the remaining tensions between privacy, data protection, cyber security and law enforcement, and asked whether they are combinable, despite the incompatibilities that still exist, and what conflicts of law between the GDPR and other regulations (on the European level, globally, or on a transatlantic level between the EU and the U.S.) are developing. Since the debate has not been closed by this conference, it may be a good starting-point for further discussions. In particular, the governance aspects of cyber security and privacy deserve more attention, and the focus should be on discussing what the intentions of the numerous actors are, what lessons can be drawn from past experiences in this area, and what conclusions have been arrived at by relevant fora, such as the IGF.

Regarding cyber security, future debates should consider how liability could be made a reality under U.S. and EU legislation, which involves a continued, more general discussion on the value of data too. Assessing and determining the value for different types of data might not only be the basis for an appropriate risk assessment and for workable insurance schemes for damages in cases of data loss, theft or other incidents violating privacy rules or cybersecurity, but could furthermore allow for establishing general rules on data economy, including antitrust and market concentration.

Another major aspect of cyber security, which also relates to data protection discussions, is certification. With regard to cyber security, the question is whether a certification regime or different regimes could be developed. In the EU, legal initiatives like the 'EU Cybersecurity Act' proposed by the European Commission and the recent EU NIS Directive point in such a direction. What remained unclear in the conference, however, was whether there are parallel developments in the U.S. and beyond—for instance, through the design of ISO standards—and whether a common (possibly global) approach is possible.

From a practical perspective, flexibility for enhancing the security of technology is required, depending on the product and function or service provided. Bringing together affordability and security is thereby a central task in the future secure development of products. How best to achieve this was left open in the discussions.

As a specific example of the security of information on computer software security vulnerabilities, and more specifically their withholding or disclosure, the U.S. Government recently introduced the Vulnerability Equities Process (VEP), which is of especial relevance for law enforcement purposes. In the EU, Germany has established an agency with a similar task, the Central Authority for Information Technology in the Security Sphere (ZITiS), which has been set up to assist (national) intelligence agencies in an-

alysing data and communication as well as lawful hacking while only providing tools and not carrying out the analysis itself (https://www.lawfareblog.com/germanys-crypto-past-and-hacking-future). However, as this aspect was merely touched upon at the conference and the concrete implications of these approaches are still being debated, it requires further discussion.

Another practical, pressing issue has been the steady evolution of the internet of things. As this is one of the main challenges for cyber security and data protection today, the discussants outlined various issues that need to be tackled. But so far, no common approaches on how to address possible problems existing on either side of the Atlantic have been developed by single states. So, this topic needs to be discussed more comprehensively.

In the course of the discussions, attendees also focused on the current tendencies of data localisation that can be recognised in various countries around the globe. While this has some positives, the participants mainly highlighted some of the associated disadvantages, such as the suppression of the free flow of data. In particular the question of whether data localisation can lead to better data security has been the subject of a controversial debate which calls for deeper investigation. On a more general level, an analysis should be made of how to cope with this practice not only in transatlantic relations but also on a global scale.

Another critical point of debate was the role of the markets in the EU and the U.S. In this the discussants recognised an uneven development. While the U.S. market has been characterised as strong, including some of the major players in the internet economy, the participants pointed out that there was room for further development in Europe. In particular the insurance market has been a controversial issue: in addition to the unfavourable focus on post-breach actions and measurements, the discussants stressed the future task of creating benchmarks and defining best practices, which should also include the elaboration of a global framework.

In the light of recent important cases brought before the courts, the contributions and discussions emphasised that court decisions in both the U.S. and the EU play a vital role in shaping the cyber security and data protection landscape. Notably the Microsoft Corp. v. United States case lodged with the U.S. Supreme Court in 2017-2018 raised significant questions. On the one hand, one wonders what the long-term effects of the recent or ongoing legislative initiatives in the U.S., such as the new Clarifying Lawful Overseas Use of Data Act (CLOUD Act), may be. On the other hand, deeper analysis is necessary to determine the potential implications of the case for the relevant actors in Europe —for instance, what may follow from these developments for the European courts, DPAs, or other law enforcement authorities. On April 17 2018, the Supreme Court declared the Microsoft case moot because its warrant had been replaced by the warrant of the new CLOUD Act. The debate on the access of law enforcement authorities to data is nevertheless still crucial. However, courts have recently started to interact more closely:

in this respect, the participants pointed to the concept of the 'dialogue of the judges' in which single European constitutional courts monitor what other constitutional courts in the EU are doing and refer to or include their rulings in their own, which can enhance the overall coherence of law. However, this issue requires further discussion as it remained unresolved at the conference.

A more general point raised in the discussions was the necessity to bring together still largely self-referential discourses in different disciplines —for the sake both of academic debates and of the need to find common approaches to practical issues.

In conclusion, as can be seen from the variety of issues addressed and the results of the conference, the field of privacy, data protection, and cyber security contains many potentially fruitful avenues for future discussion. The contributions of the first conference led to important findings, and open questions as well as new developments can be a sound starting-point for the next.

ACKNOWLEDGEMENTS

The organisers would like to thank all the conference participants for making it such a great success. It was the invaluable inputs of both the speakers and the attendees which ensured such productive discussions. We are particularly thankful to all the speakers for their extra efforts in revising —and at times extending and deepening— their talks for publication in this edited volume.

A stimulating Keynote of Michael Weidner, Professor for Security in Information Technology, Technical University Darmstadt, and Director of the Fraunhofer SIT, Karlsruhe, on "Cyber Security and Data Protection – Friends or Foes?" at the opening session, and a fascinating Dinner Speech by Karsten Geier, Head of Coordination of Cyber-Policies, German Foreign Office, Berlin, on "Transatlantic Cooperation in Cyber Security and Privacy Issues" set an excellent frame for the discussions at the conference, and we would like to express our greatest gratitude for their time and readiness to share their thoughts with us.

Similarly, our thanks go to all who did outstanding work in so smoothly organizing this conference, especially those working behind the scenes, Christian Marks, and Luis Oala and the entire HIIG management team.

Many thanks also to all who excellently contributed to finalizing this edited volume, especially Andrew Hendry for language revision and copy editing.

This conference would not have been possible without the generous support provided by Facebook, for which the organizers are especially grateful.

U.S. AND EUROPEAN CYBER SECURITY AND PRIVACY POLITICS AND STRATEGIES: THE CHALLENGES AHEAD

Privacy and Cyber Security on the Books and on the Ground – An Overview

ZACHARY K. GOLDMAN

I think the importance of the discussion is obvious, but it should not be underemphasised that the EU-US relationship generally, and within that framework the German-US relationship, is the most important in the world —the most important in the world in terms of security issues and the most important in the world in terms of commercial and economic issues. Data privacy and cyber security is an area where these two sets of issues intersect, and so I think it is no exaggeration to say that these questions are among the most important on the EU-US and German-US agendas. Consequently, I suppose, any attempt to achieve greater understanding among scholars and leading practitioners on both sides is of great strategic importance, and so I thank you all warmly for coming today.

I thought it would be useful to frame the discussion around four core themes, which I hope and expect to learn a lot about over the next two days, as we speak together. The first theme is the relationship among a few core concepts that exist as distinct bodies of law and policy in the US and which, my instinct tells me, also exist as distinct bodies here, although, perhaps, to a lesser extent. These core concepts are data privacy, cyber security, foreign intelligence surveillance, and law enforcement surveillance. And I would argue that these four concepts are, as I said, distinct bodies of law and practice in the US, each of which is governed by a rich statutory regime and is obviously in dialogue with the others. A lot of attention has been paid in the last few years to the relationships between privacy and foreign intelligence surveillance, and privacy and law enforcement surveillance. I think that perhaps a less well-understood dynamic is the relationship between privacy and cyber security, and the extent to which these are distinct or perhaps overlapping fields of law and policy. The real question then becomes: how much overlap is there between data privacy and cyber security? To what extent should these two phenomena be understood as serving distinct strategic objectives, with distinct sets of values and distinct sets of regulations, or, conversely, as being two sides of the same coin? And, of course, I certainly have thoughts about what that relationship looks like in the US perspective. But hearing from all of you about what that relationship looks like at present in the EU, particularly given the imminent entry into force of the GDPR, will certainly be important for us over the next couple of days.

The second theme consists in a significant question which is more at a theoretical or abstract level. The differences between the US and the EU over the understanding of privacy are clear at this theoretical level: in the EU, privacy is a fundamental right; in

the US, I would describe it as a value among many other values, including individual autonomy, economic freedom, and national security —all of these are values that we in the US hold dear and that are reflected in our laws and policies, and are sometimes traded off against one another. A persistent question —to which I do not think there is an answer, but which I think is a question that persistently begs to be asked— is: what difference does this distinction between privacy as a fundamental right and privacy as one of a number of different values actually make? Is it really significant that privacy is considered a fundamental right in the EU, whereas in the US it is considered a value, with robust constitutional and statutory protection, and robust institutional protections?

As a third theme, we need to consider the following: as a compliance matter, the subject of this workshop has been carefully worded as 'Privacy and Cyber Security on the Books and on the Ground', and so as a matter of compliance for companies that own the data and the networks and that are legally responsible —at least in the US— for protecting the data and the networks, what impact do these differences —both at a theoretical level and as a matter of regulation— have on the actual behaviour of companies with regard to the collection, storage, processing, and use of data in a variety of contexts? In other words, what are we actually talking about here? What is the impact of these regulatory and theoretical distinctions 'on the ground'?

As for the fourth theme, I think it is becoming increasingly important both in the EU and in the US to ask questions about the responsibilities and obligations of internet platforms, and also to ask a series of questions which are really in dialogue with each other. So, we are well accustomed to asking questions about the privacy obligations of internet platforms. That is a mature discussion —both in the EU and in the US. We are starting to ask about the security obligations of platforms. I have had fascinating conversations with people working at some of these companies who really have a vision of the role that they can play in internet security as a general matter, as the network continues to scale up and reaches the next billion customers. But we are also facing a number of other challenges with regard to the role of internet platforms. In the US some of these challenges have robust statutory regimes to help manage and govern them. I am thinking of copyright control and controls on the spread of child pornography —each of these areas of law in the US is reasonably well developed; there are institutions that support them, processes within companies to manage them, and the like. But there are many other challenges that we are only just beginning to think through. So, for example, what do we think of terrorism-related content on the internet, radicalisation and recruitment on the internet, hate speech, fake news, cyber bullying, self-harm, and revenge pornography? All of these are content-related harms that take place on internet platforms, and we are engaged in a robust debate about what the role of the platforms in policing these harms should be. And I think, in this respect, it is important to ask the question about the relationship between the governance of these content-related harms, what we ask companies to do with regard

to privacy and security, and what companies have demonstrated they are able to do in terms of policing compliance with their own terms of service. And these are three, I think, distinct but closely related challenges for internet platforms moving forward.

Furthermore I suppose, although it is not entirely clear how, my instinct is that these three areas are strongly interconnected, and that what we ask of companies to do in one area will have an impact on what they are able to do, and more importantly, expected to do in the others. And I think at least with regard to US law, there are important statutes that provide immunity in some contexts, that have limited —by design— what the platform companies want to do in terms of policing content on their networks. And that may impact on what they have been able to do with regard to certain other challenges.

So, these are four, if you like, high-level thoughts about questions we may seek to ask or at least have in the back of our minds over the next few days. We are most grateful that you have been able to come, and I look forward to learning an enormous amount from you and to continuing our dialogue —so, thank you very much.

Preliminary thoughts on a comparative analysis of the relationship between data protection, privacy and cybersecurity law in the EU and the US

PAUL NEMITZ[1]

Data protection, privacy and cybersecurity law in the EU are all complex subjects in their own right. Discussing them together, looking at links, possible synergies and possible incoherence increases the complexity of the analysis. Doing this in a transatlantic, comparative perspective makes it twice as complex, to say the least.

When embarking on an exercise of such complexity, it is important to start with the basics and not to become entangled in technicalities too early. Data protection law in Europe is not only a complex and technical matter. The General Data Protection Regulation[2], and the Directive on data protection in the police and the judiciary[3], which both come into effect on 25 May 2018, serve to realise for citizens a fundamental right (Art. 8 of the Charter of Fundamental Rights of the European Union) on the level of constitutional, primary law. And the fundamental right to privacy (of communications) (Art. 7 CFR) is served by the Directive on privacy and electronic communications, soon to be replaced by a regulation[4]. These fundamental rights are becoming ever more important in the digital world in which power, public and private, is increasingly based on the collection and processing of personal data and on intrusions into privacy on a massive scale. It is an essential condition of constitutional democracy that people can control private

[1] The author expresses his personal opinion and not necessarily that of the European Commission.

[2] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation, OJ L 119, 4.5.2016, pp. 1–88, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679.

[3] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ L 119, 4.5.2016, pp. 89–113, ELI: http://data.europa.eu/eli/dir/2016/680/oj.

[4] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) ELI: http://data.europa.eu/eli/dir/2002/58/2009-12-19, as amended, see https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02002L0058-20091219; proposal for revision presently under negotiation in the European Parliament and Council, see COM (2017) 10: European Commission Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), https://eur-lex.europa.eu/legal-content/EN/HIS/?uri=CELEX:52017PC0010.

and public power rather than private and public power controlling people through the unlimited collection and processing of personal data. Therefore, the need to rigorously defend the fundamental rights under Articles 7 and 8 CFR is increasing in the digital age.

This being said, the fundamental rights to privacy and protection of personal data under Articles 7 and 8 of the Charter of Fundamental Rights of the European Union have of course to be balanced with other fundamental rights and with important public interests, such as the interest in security and cybersecurity. The aim must be the practical concordance of fundamental rights as well as their protection combined with the attainment of other important public interests, such as security and cybersecurity. Any limitation on a fundamental right must, according to the first sentence of Article 52 (1) of the Charter, be provided for by law and respect the essence of the right. We have already learnt from ECJ jurisprudence that a permanent and general surveillance of the content of communications for purposes of security (and I would say for any purposes) does not respect the essence of the fundamental right to privacy, and is thus forbidden[5]. Furthermore, according to the second sentence of Article 52 (1) of the Charter, limitations on fundamental rights must be proportional and may only be introduced if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others. Again, a clearly worded ruling by the ECJ states that a permanent and unlimited collection of metadata on telephone calls, of the type 'who called whom at what time and from where', is not proportional and thus illegal under EU law[6]. This derives from the principle that in a free society, the means of communication must in principle be free from surveillance. This principle also applies to other forms of communication than telephone calls, e.g. e-mails or the use of the internet and internet messengers.

Security in the overarching sense is served on the one hand by law enforcement and on the other by the preventive work of intelligence services. There are of course broad conditions of security relating to the economy and social cohesion, tolerance, dialogue, integration, education, and so on. And not all cybersecurity law falls within the scope of the broader category of security law. We are also confronted with an important body of technical, public law rules for cybersecurity, which prescribe certain technical or behavioural rules, without providing a basis for sanctions or intervention for either criminal law enforcement or intelligence services[7]. This specific public law element, in addition to the traditional security-related duality between criminal law and intelligence law, further

[5] Digital Rights Ireland and Others, C-293/12 and C-594/12, EU:C:2014:238, paragraph 39; and Maximillian Schrems v Data Protection Commissioner, Case C-362/14, paragraph 94, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62014CJ0362.

[6] Digital Rights Ireland and Others, C-293/12 and C-594/12, EU:C:2014:238.

[7] For an overview of legislation and related reform plans see: https://ec.europa.eu/digital-single-market/en/cyber-security https://www.enisa.europa.eu/events/enisa-cscg-2017/enisa-cscg-2017-agenda.

increases the complexity. Law enforcement and intelligence services may have an interest in these bodies of law. But these bodies of cybersecurity law do not belong to the classic bodies of criminal law or intelligence law, are not part of national security law and therefore clearly fall within the competence of the EU. Beyond that, it is a misunderstanding to believe that due to the exception of Article 4 (2) EU Treaty, which reserves national security matters to Member States, EU institutions have no say when it comes to matters of national security: Union institutions must be able to control the application by Member States of this exception and its variants in secondary law. The application of the exception is subject to the principle of necessity and proportionality as well as motivation in order to guarantee judicial review[8]. The Commission and the data protection authorities must be able to assess the adequacy of access to personal data for national security purposes in third countries, as happens in the context of the Privacy Shield[9]. And the Fundamental Rights Agency reports on the law of intelligence and surveillance in Member States in the light of the Charter of Fundamental Rights. Another point that should be noted is that the European Convention on Human Rights does not contain a national security exemption and the European Court of Human Rights in Strasbourg thus reviews the compliance of Member States with the Convention also in relation to national security[10].

In national criminal law and criminal procedure, as well as national intelligence law, we find provisions of interest to cybersecurity. In the EU, to make matters more complicated, these are provisions of national law, based on the distribution of competences between the Union and its Member States, and in some cases on specific empowerments in EU law[11]. Both law enforcement and intelligence law traditionally allow for deep intrusions by the state into human rights and, as we call them in the EU, fundamental rights. That is why in these areas of law the defensive function of fundamental rights and human rights against the state is so important. The key location of fundamental rights in criminal law is the law of criminal procedure, with particular importance given to the rights of the defence. Any intrusion into fundamental rights, from eavesdropping through to detention until sentencing, is under the control of a judge and must be challengeable ex ante or ex post.

[8] On this point see, for example, ECJ ZZ v. Secretary of State for the Home Department, C-300/11; ECLI:EU:C:2013:363.

[9] Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield (notified under document C(2016) 4176) OJ L 207, 1.8.2016, p. 1–112 (ELI: http://data.europa.eu/eli/dec_impl/2016/1250/oj; on this see also the ECJ in Schrems v. Data Protection Commissioner.

[10] See an overview of ECHR case law on national security at https://rm.coe.int/168067d214.

[11] For an overview relating to intelligence services, see the three reports by the European Union Fundamental Rights Agency in Vienna, an EU body, at http://fra.europa.eu/en/publication/2015/surveillance-intelligence-services.

In intelligence law, on the other hand, one of the major issues today on both sides of the Atlantic —which in Europe is reflected in the very detailed jurisprudence of the European Court of Human Rights[12]— is to establish the principle that in a democratic state which exercises power under the rule of law and in respect of fundamental rights, there can be no broad empowerments for uncontrollable action for Intelligence services and also there can be no actions by state authorities which cannot be subject to judicial or quasi-judicial scrutiny ex officio and based on the exercise of rights by individuals. Intelligence services have become used to an unacceptably low level of challengeability and scrutiny. At a time when intelligence work is intruding more and more into the individual rights of more and more people simply because the technologies and the internet as a two-way medium make this possible, and at a very low budgetary cost, judicial or quasi-judicial scrutiny has to increase in parallel. Without such a parallel increase in intensity and depth of control, triggered ex officio and by individual challenges, the zones free of scrutiny in intelligence services would increase in line with technological developments, which for constitutional democracies is untenable. It simply cannot be accepted under the constitutional settlement on either side of the Atlantic that new technology should undercut the rights of individuals or the division of power in constitutional democracies. Let us be very clear here: if in parallel with the increased technological capabilities of law enforcement and intelligence services there is no increased scrutiny and control, freedom and democracy are in danger because this unchecked increase of technological power in executive services constitutes a real power shift away from parliaments and the judiciary, which traditionally protect people against the overreach of the state, each with different legal instruments and different legal and constitutional functions. The ECtHR's jurisprudence in Europe, as well as the discussions relating to the post-Snowden reform efforts in the US pertaining to the introduction of judicial scrutiny ex ante (but without contradictory procedures for the individuals concerned), the strengthening of the mandates of Inspectors General and the introduction of an Ombudsperson, all demonstrate the importance of this issue[13].

Before all this, it is very important that the academic and journalistic scrutiny of law, technologies and the practices of intelligence services in particular —the least transparent and at the same time the most advanced users of technology— should be intensified. Without such intensified scrutiny in public fora and the related intellectual work, it will become increasingly difficult for the judiciary and parliaments to exercise their control functions over the highly technicised executive functions. While digital technologies are

[12] For an overview of ECtHR jurisprudence on national intelligence and mass surveillance see: https://www.echr.coe.int/Documents/FS_Mass_surveillance_ENG.pdf.

[13] See with further reference the Art. 29 Working Party review of the EU – US Privacy Shield, WP 255 of 28 November 2017.

increasing our access as individuals to information in a truly marvellous manner, at the same time these new technologies are being increasingly developed and used under a veil of secrecy and their functions and impacts are understood only by an initiated minority. We need open sources and open standards not only in technology for commercial use but also for the state, and in particular for the functions of the state, which are highly intrusive into fundamental rights and risky in democracy and thus require intense scrutiny and constant control.

The key here, as with all academic work on the law of the internet and digital data, is that we need a holistic understanding of the capabilities of technologies, their use and impacts and how they develop in parallel to an understanding of the law. It is not only important to have an up-to-date understanding of the threats to freedom and fundamental rights that are posed by these ever more powerful technologies and of the ways in which they are used. It is also important because only technologically neutral legislation can actually keep up with the high speed of technological development. But the very nature of technology neutral legislation, such as the GDPR and the Directive on the protection of personal data in police and judicial cooperation, is that with the progress of technology the real meaning and relevance of the legislation also changes. This is so because the whole purpose of technology neutral legislation is that it should retain its relevance through an adaptation of its interpretation and thus meaning as technology progresses or even as new technologies arise. This in turn, however, means that lawyers and judges can only give the interpretation required by the times to the technology neutral legislation if they understand the technologies, their use and impacts, to which they are required to apply the law.

Some claim that the ECJ in its key judgments on data protection has neither understood the technologies nor the realities of the underlying operating and business models[14] or the realities of security services' operations or related US law[15]. The opposite is true: there is a clear logic and coherence in the series of judgments issued by the ECJ shaping the rules for the internet and digital technologies. It is fair to say that it is the ECJ, through its jurisprudence on the internet and digital technology, that has become the world leader in the judicial shaping of the digital domain along a number of coherent lines. These lines are basically that freedoms and fundamental rights cannot be undermined by technology, and in particular that there is no question of absolving technology and its functioning of

[14] Google carried out hearings in many EU capitals following the ECJ "Right to be Forgotten" ruling (Google v. Spain, ECLI:EU:C:2014:317), pretending that the ruling was impossible to enforce, https://static.googleusercontent.com/media/archive.google.com/en//advisorycouncil/advisement/advisory-report.pdf. See also https://www.independent.co.uk/life-style/gadgets-and-tech/news/right-to-be-forgotten-google-accused-of-deliberately-misinterpreting-court-decision-to-stoke-public-9582985.html.

[15] Robert Litt in FT of 5 October 2015: 'Europe's court should know the truth about US intelligence'.

responsibility, even if the technology runs and develops autonomously[16]. Also, there must be limits to the empowerments given to law enforcement and intelligence services to use technologies, particularly in respect of the mass or bulk collection of personal data[17]. It lies beyond the scope of this paper to detail the other judgments of the ECJ and ECtHR that pre-date and post-date the cases referred to here, and which all together demonstrate not only a good understanding of the technologies as they develop and the legal and factual realities of their application, but also wise judgement in the need to rethink the responsibilities of those using technologies and the respective rights of individuals in the light of new technological capabilities.

Data security is a necessary component of data protection and privacy because the protection of personal data is not possible without keeping data safe, and it is actually an obligation under existing and future rules in the EU to maintain data security for the purpose of data protection. Non-compliance with this important obligation of 'security of processing', laid down in Art. 32 GDPR, can be fined, in the case of a private actor, up to a total of 2 per cent of their global turnover, according to Art. 83 (4)a GDPR, and if the non-compliance relating to the security of processing is in contravention of a specific order of a supervisory authority under Article 58 (2) GDPR, up to a total of 4 per cent, according to Art. 83 (6) GDPR. It is important to note in this context that the 'security of processing' referred to in Art. 32 GDPR covers the transmission of data, as 'processing' includes transmission as defined in Art. 4 (2) GDPR. We thus see that data protection law in Europe actually serves important concerns of cybersecurity.

Between the US and the EU there are differences in the interpretation of different terms. In the EU, data protection (Art. 8 Charter) is a right distinct from the right to privacy (Art. 7 Charter). In fact, data protection law protects not only natural persons but also data in the public domain, insomuch as the data identify or make it possible to identify an individual. In Europe, rules on privacy protection, such as the E-Privacy Directive, also protect legal persons, although they only protect communications which are made in private, thus not data in the public domain. In the US, the word 'privacy' is used without such a distinction also for data protection, which confuses the matter.

[16] Google v. Spain, c-131/12, ECLI:EU:C:2014:317, paragraphs 22 and 32ff.

[17] On law enforcement see the ECJ case Digital Rights Ireland Ltd v. Minister for Communications, ECLI:EU:C:2014:238; on intelligence services see the ECJ Schrems case, ECLI:EU:C:2015:650.

Each of the areas of law touched on so far is opening up domestically, and when I say 'domestically' in Europe I am not talking about the complexities between EU law and national law, which are very complicated questions and a subject of jurisprudence at the highest level in Europe. This jurisprudence, as far as the protection of individual fundamental rights is concerned, is split between three jurisdictions, namely the national constitutional courts, the European Court of Justice, and the European Court of Human Rights, a court which from outside the national jurisdictions, from outside the countries, controls states' actions and their relations with their citizens. The European Court of Human Rights allows appeals from individuals once they have exhausted domestic remedies to protect their fundamental rights as they are set out in the European Convention of Human Rights —in addition to national catalogues of fundamental and human rights, which exist in many, but not all, of the EU Member States, and which are applied and enforced by the national constitutional courts. The EU Court of Justice can only act when EU secondary law is at issue or when it controls the actions of EU institutions, and it checks actions in these contexts against the European Union Charter of Fundamental Rights. The details of interaction between these three jurisdictions and the three catalogues of human and fundamental rights are quite clear. Suffice it to say that all three bodies of law and jurisdictions complement but also influence each other, their interaction at the best of times being a wonderful example of enlightenment and constructive judicial dialogue in action, while at other times an example of rather contrarian behaviour. The positive fallout of having three jurisdictions entrusted with the protection of fundamental rights is, however, a race for supremacy in the sense that each of the jurisdictions is keen, or pressured, to demonstrate that it is a better, or at least no less good, protector of fundamental rights than any of the other two jurisdictions. Europe and its people benefit from the dialogue of the judges in these three jurisdictions and also from the occasional competition they enter into.

RESPONSIBILITIES, RIGHTS AND ENFORCEMENT

The Relations Between Cybersecurity, Data Protection and Privacy: A European Perspective

THÉODORE CHRISTAKIS

From a European perspective, cybersecurity and human rights seem to mutually reinforce each other. Recent instruments, such as the GDPR or the NIS directive, require States to implement a series of technical, procedural and organisational measures to enhance the security of networks and data and promote a culture of risk assessment, cybersecurity and incident response and reporting. The EU's 'cybersecurity package' announced in September 2017 could also have a positive impact in this respect by promoting concepts such as 'security by design' or a responsible management of vulnerabilities. Last but not least, the ePrivacy Regulation, currently under discussion, is designed to complement the GDPR and could, in some respects, have an important impact for the promotion of both users' rights and cybersecurity. The draft adopted a few days ago by the European Parliament notably includes a requirement for EU Member States to promote and even make mandatory the use of end-to-end encryption while refraining from requesting ICT actors to use 'backdoors' or other measures that could result in the weakening of the security of their networks and services. It remains to be seen if this provision will survive the expected reaction of some States who consider that there is a necessity to strike the right balance between cybersecurity, human rights and the need for effective intelligence and law enforcement through cyber-surveillance in order to protect a number of important legitimate aims, such as national security and crime prevention.

This brief paper intends to offer a European perspective on the relationship between cybersecurity and human rights. I will argue here that cybersecurity and data protection are friends from a European perspective, not foes. In order to do this, first of all, we have to ask ourselves what we mean by cybersecurity. This is very important because so many definitions of the term exist. When I took a look at the definitions of cybersecurity given by different States, the briefest definition of all was that provided by Norway, which defines cybersecurity as 'The protection of data and systems connected to the internet'. So if we take Norway's definition, the protection of data means the protection of cybersecurity. Another example is the definition of cybersecurity by Australia: 'Measures relating to the confidentiality, availability and integrity of information that is processed, stored and communicated by electronic or similar means'. And according to the Oxford Dictionary, cybersecurity is: 'The state of being protected against the criminal or unauthorised use of electronic data, or the measures taken to achieve this'. So, all these definitions and several others that exist clearly show that cybersecurity does not mean cyber surveil-

lance. Indeed, measures of cyber surveillance could be detrimental to cybersecurity and to privacy— through the use of backdoors and, to a lesser extent, encryption— and all of these things could weaken cybersecurity. Some States indeed use the argument that cyber surveillance is necessary in order to limit human rights and data protection. For instance, tens of thousands of Turkish citizens were detained or dismissed from their jobs in 2017 on the grounds that they had downloaded an encrypted messaging app. However, cybersecurity cannot be used as a kind of Trojan horse in order to erode civil liberties, starting with the protection of data, the right to privacy and respect for correspondence. The ECtHR and other human rights treaty bodies constantly emphasise that the police must exercise 'their powers to control and prevent crime in a manner which fully respects the due process and other guarantees which legitimately place restraints on the scope of their action to investigate crime and bring offenders to justice'. Furthermore, in a similar way the UN GGE emphasised that if States need to 'cooperate to prevent harmful ICT practices and should not knowingly allow their territory to be used for internationally wrongful acts using ICT', they should, in doing so, 'also guarantee full respect for human rights, including privacy and freedom of expression'.

Some scholars have gone as far as saying that cybersecurity should be recognised as a human right. In the EU Charter of Fundamental Rights we have two distinct articles, Article 7 and Article 8. The first one is on the respect of privacy, the second on the protection of personal data. And from a European perspective, cybersecurity and human rights seem to reinforce each other. I think that from a European perspective, better privacy means better cybersecurity, and better cybersecurity means better privacy. I will try to present five points in support of this idea but let me first say a few words about the architecture of cybersecurity and data protection in the EU because both of these concepts are related to the idea of a Digital Single Market. The Digital Single Market is comprised of several things, and includes two big pillars: digital privacy and data protection on the one hand and cybersecurity on the other. So, in the digital privacy pillar, we have important legal instruments such as the GDPR and the ePrivacy Directive. As you know, the GDPR ensures that personal data can only be processed under strict conditions and for legitimate purposes and must be processed in a way which would not be abusive. The proposal for an ePrivacy Regulation, currently under negotiation (as part of a more general process to replace old directives with regulations), intends to protect the security of communications, privacy and respect for the fundamental rights of people who are communicating, regardless of the technology that they are using. And then we also have the cybersecurity pillar with other instruments that are very important, such as the NIS Directive on the security of network and information systems. And one and a half months ago, the EU announced a big cybersecurity package with numerous important instruments, including an important regulation on the EU certification framework. So, how do all of these things mutually reinforce each other? Let me answer in five brief points.

First of all, the obligation to implement appropriate technical and organisational measures to protect personal data. This is very clearly stated in Article 32 of the GDPR and what is interesting, of course, is that we ask States and companies to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, but we don't tell them how, we don't impose any obligation of results. This is a classic due diligence obligation where we let the companies decide and they can choose what means to adopt. You can choose: in Article 32 many different means are suggested, such as certification, encryption, a process of regular testing, using approved codes of conduct, approved certification mechanisms etc. So, you have a list, but you have the choice of means, you can choose what you want. And what you need to do is to show that you have adopted a strong stance on cybersecurity in order to protect data, and not only you for there is another Article —Article 28— which requires that if you use third-party processors, you must ensure that they provide sufficient contractor guarantees on the same issues. So, from this point of view, it has rightly been said that the GDPR will 'raise the benchmark of the quality of cyber security controls', partly because of the heavy fines that companies will eventually face if they do not comply with the requirements of the Article. And, of course, one could say that you have no obligation of results but only an obligation of means. On the other hand, this is logical, this is how due diligence works, and the duty, the burden, is on companies to assess and decide what they will have to do, in the knowledge that they have to do it, and they have to prove in the case of a problem that they have followed the best practices, taking into account all parameters in order to avoid the risks of a data breach. And, in the same field of implementation of technical and organisational measures, we also have the NIS Directive, which must be implemented at the same time as the GDPR, which has the same requirements concerning the operators of essential services and digital service providers, which have similar obligations. And we also have the forthcoming ePrivacy regulation which will do the same thing concerning the protection of information stored in and related to a user's terminal equipment. So, this is a whole package with the same objectives.

The second point concerns the obligation to conduct DPIAs (data protection impact assessments) on the basis of Article 35 of the GDPR. If you conduct a privacy impact assessment, which is a major pillar of the GDPR, you have to analyse a large number of things, including cybersecurity issues. This is a risk management, and when you conduct the privacy impact assessment, there is a strong component which involves demonstrating that appropriate measures have been taken to ensure compliance with the Regulation, including on the technical level, and including the 'intruder problem', the problem of the insider who might access and leak the data. So you have to take this into consideration and propose solutions, such as anonymisation or other solutions that will help deal with this problem.

The third point concerns the positive effect of the notification obligation. In the GDPR we have an obligation that personal data breaches must be notified to the relevant supervisory authority no later than 72 hours after the data controller becomes aware of it. And you have a similar obligation in the NIS Directive, which also imposes a duty on companies to report cybersecurity breaches to the relevant competent authority. And if I may add, we have in EU law other obligations of notification, for example in the eIDAS Regulation, which is about electronic identification and trust services and tries to ensure safe access to services and transactions online. So we have plenty of obligations of notification. And sometimes, in a manner of speaking, we are really 'lost in notification' —we might wonder how companies could cope with this situation. And it is very interesting that, for example, in France, the Data Protection Authority has mapped out notification obligations so that each time a breach occurs, the company concerned is informed which authority it should notify, depending on the kind of breach that has occurred. For example, if there is a problem for cybersecurity and personal data, you must notify both the Data Protection Agency (CNIL) and the National Cybersecurity Agency (ANSSI). And this could be mutually reinforcing. Now some scholars have talked about the risk that this 72-hour GDPR notification deadline could lead to security breach cover-ups because companies might be unwilling to report, and they would be willing to avoid the fine for late notification. I think that these fears are exaggerated. In reality, this notification requirement is a positive thing for cybersecurity and I think that in the USA there is an important culture of notification procedures. In France, cooperation between the CNIL and ANSSI, the national cybersecurity agency which is —unlike the situation in other countries— outside the intelligence community, could prove helpful in dealing quickly with data breaches occurring as a result of cyberattacks.

Point four: the relation between privacy-by-design and security-by-design. The GDPR provides that any product or service is to be designed from the very beginning with data minimisation standards in mind, and at the same time the whole cybersecurity package has been announced, including the regulation on the certification framework, which tries to provide for security-by-design, which means that products (including IoT) should be manufactured using state-of-the-art security development methods and following sufficient security testing, and also that companies should update their software in the event of newly discovered vulnerabilities. So, we have here two concepts that are closely connected: privacy-by-design and security-by-design.

Finally, my last point: encryption and backdoors. A few days ago the EU Parliament adopted the draft of the ePrivacy Regulation, which includes the following paragraph:

> In order to safeguard the security and integrity of networks and services, the use of end-to-end encryption should be promoted and, where necessary, be mandatory in accordance with the principles of security and privacy by design. Member

> States should not impose any obligation on encryption providers, on providers of electronic communications services or on any other organisations (at any level of the supply chain) that would result in the weakening of the security of their networks and services, such as the creation or facilitation of 'backdoors'.

We will see if this is able to overcome the resistance of several States, including France —let us not forget that there have been some reactions, and several authorities, especially in the law enforcement and intelligence communities, have tried to combat strong encryption. Recently in the United States, I think a few days ago, the Deputy Attorney General came out and talked about 'responsible encryption', including the idea of promoting backdoors. In Europe it is interesting to note that at the very moment that the European Parliament was adopting the ePrivacy draft, the EU Commission was including in another legislative package —the anti-terrorist package— the idea that we must make it easier to crack encryption, while ruling out backdoors. There are some proposals in this package that I could present to you afterwards, including the idea of promoting the decryption capabilities of Europol or the idea of a structural dialogue with the industry —although we do not really know what this means— but still the idea is that we should not use backdoors. Despite this precaution, it is interesting to note this divergence between the 'human rights' EU organs that wish to 'promote' the use of end-to-end encryption and the 'anti-terrorism' work of the EU, which has expressed reluctance about strong encryption.

As a conclusion it seems to me that, from a European perspective, cyber-security, data protection and privacy appear, from several points of view, as mutually reinforcing each other. While data protection and respect of privacy are already codified in two distinct articles of the EU Charter of Fundamental Rights, this Charter does not include a fundamental right to cybersecurity. We could nonetheless wonder if the close relationships and interactions between the three concepts could lead to an evolution in this field in the future and if a fundamental right to cybersecurity could emerge progressively in the future in the "penumbra" of articles 7 and 8 and the relevant secondary legislation of the European Union.

Some Concerns with Privacy as A Framework for Cybersecurity

RANDAL S. MILCH

Professor Christakis and I are to discuss the question 'Cyber Security: Public Responsibility and Fundamental Rights or Shared Responsibility and Regulatory Challenge?' As I read the question posed, it is designed to shed light on which might be a better overall legal and regulatory framework: greater governmental command and control or a regulatory solution that encourages greater private sector responsibility. This is a hard question (as it should be) but there is an important assumption lurking in the question that I do not believe is true: the public value to be protected by enhancing cybersecurity is the 'fundamental right' to privacy. Privacy is of course a vitally important value. But before 'privacy' becomes the foundation from which we make government attempts[1] to enhance cybersecurity, we should have confidence that this approach is likely to lead to cost-justified improvements in cybersecurity. Little about our current approach to privacy leads me to think that this will be the case.

It is important to keep in mind the complexity of the cybersecurity problem. It has at least four parts: (i) a wide variety of information about a data subject; (ii) in the possession of a data holder (a data collector, processor or both); (iii) is stolen by a data thief; (iv) due in part to a vulnerability in the information security of the data holder.

This attempt at a neutral statement of the problem masks a good deal of variety in each component. The information at risk may be provided by the data subject directly to the data holder or generated by the internal processes of the data holder as part of a service or product provided to the data subject, or purchased by the data holder. The data at risk also may be scooped up by the data holder from the digital wild, freed there by the subject for her own reasons. Any piece of information regardless of origin may itself be innocuous but a compilation of public and private data may become shockingly intrusive if the data holder has the proper capabilities. A data thief may have a range of motives and capabilities: hacktivist, criminal profiteer, nation state warrior. And finally the vulnerability exploited can range from obviously poor cyber-hygiene to susceptibility to a sophisticated zero-day attack wielded by a nation state.

[1] I use 'government attempts' in a very broad sense. I would include new cybersecurity legislation designed to enhance privacy, cybersecurity regulatory actions that have better privacy as their goal, and private actions —whether based on statute, regulation or common law— that seek to compensate the cyber-breach victim for her loss of privacy.

In this complex context, a cybersecurity legal regime should have three basic goals: to provide data subjects with both better information and the impetus to take steps to protect their data through the choices they make; to provide data subjects with compensation commensurate to the harm they suffer after a data loss; and through the first two goals, to provide data holders with clear market signals about how much they should invest in cybersecurity. I think a privacy-centric approach falls short in achieving each of these objectives.

First, let's look at the question of increasing the agency of the data subject in the fight for better data protection. Data protection is enshrined in the EU's foundational documents: 'Article 8(1) of the Charter of Fundamental Rights of the European Union and Article 16(1) of the Treaty on the Functioning of the European Union provide that everyone has the right to the protection of personal data concerning him or her.'[2] Data protection is in turn 'closely linked to respect for private and family life protected by Article 7 of the Charter.'[3]

The EU's initial effort at regulating data protection[4] has been the subject of an extensive re-write in the face of significant technological change since its adoption in 1995. The new General Data Protection Regulation, among many changes, has significantly enhanced the disclosure obligations of data collectors and processors and made the data subject's consent to collection and processing harder to obtain. Assuming a data subject reads and can understand a suitably written disclosure, the subject is on notice and can make choices relating to collection and processing and the collectors and processors are required to live up to their affirmative statements of how they collect and use data (as enhanced by legislation or regulation).

The privacy enforcement scheme in the United States is similar in concept although perhaps more contractual in nature. The Federal Trade Commission —the de facto privacy regulator for much of the US economy— regards companies that fail to live up to their privacy promises as violating the 'deceptive practices' prong of Section 5 of the FTC Act.[5] Significant civil penalties can result.[6] Again, the data holder's obligations are meant to be clearly stated and the data subject has the opportunity to choose to go forward based on the information in the policy (assuming they read and understand the policy).

[2] Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (27 April 2016) (General Data Protection Regulation or GDPR) 1.

[3] European Commission, 'Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)' at 7 (25 January 2012).

[4] 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.

[5] 15 U.S.C. §45a.

[6] Solove, Daniel J. and Hartzog, Woodrow, 'The FTC and the New Common Law of Privacy' (2014), 114 Col. L. Rev. 583, 612.

But privacy's disclosure and consent structure —in both the EU and the US— does not map to the cybersecurity landscape. Neither the GDPR nor the FTC's deception cases require a controller, processor or holder to disclose the technical measures they have put in place or seek the consent of the data subject to the security measures they have adopted. This is understandable. It would increase cyber-insecurity to require a data holder to publish the details of its security efforts. And even if they were published, it would be the rare data subject who could understand those details and make an informed buying choice. Privacy disclosures operate at a high level and concentrate on commercial issues (what the data controller will do with data it has) but fail to provide a data subject with security information with which to make a cybersecurity choice.

Data subject choice must also grapple with the elephant in the room when it comes to data privacy: the apparent absence of real interest in the problem on the part of data subjects. As the GDPR admits, '(n)atural persons increasingly make personal information available publicly and globally',[7] and do so with no apparent thought to immediate or long-term loss of privacy. Data subjects do not appear significantly to change their business habits in the wake of a corporate breach, and companies with massive breaches do not appear to suffer long term in the market. This indifference to the self-protection of personal data is clearly a difficult social problem to solve, but it has persisted even as we have increasingly looked to data holders as privacy guarantors. I see no reason to believe that doubling down on the privacy framework will drive data subject behavior toward better cyber awareness and cyber hygiene.

Turning to loss-based compensation for harms attendant to a breach, privacy is unsuitable due to the inherent indeterminacy of the value of personal data. All but one of the US privacy torts, for instance, recognize that the victim's loss of privacy is 'intangible'[8] and the damages awarded are notoriously squishy and subjective. Both nominal damages awards to unattractive plaintiffs and outsized judgments against unattractive defendants[9] are common as courts struggle with redressing 'damages that are uncertain and possibly unmeasurable.'[10]

A number of federal privacy statutes grapple with privacy's intangibility problem by establishing an arbitrary array of statutory damages, frequently without any requirement that the plaintiff prove actual harm. The Fair Credit Reporting Act, for instance, provides in the case of 'willful violations' for 'damages of not less than $100 and not more than

[7] GDPR at (6).

[8] Restatement 2d Torts §§ 652A-E. The outlier is the tort of appropriating another's name or likeness, where the measure of damages generally is the profit associated with the mis-appropriation. Id. at § 652H.

[9] The Bollea (Hulk Hogan) v. Gawker matter is a notorious example. Hogan was awarded $115 million in compensatory damages, which included $60 million for emotional distress, as well as an additional $25 million in punitive damages. After Gawker declared bankruptcy, the parties settled for $31 million.

[10] Kehoe v. Fidelity Fed. Bank & Trust, 421 F.3d 1209 (11th Cir. 2005).

$1000' without regard for actual harm[11]. The Driver's Privacy Protection Act[12], the Video Privacy Protection Act[13], and the Cable Communications Privacy Act[14] similarly require no actual harm in order to receive 'liquidated damages' ranging from '$100 a day for each day of violation or $1000, whichever is higher' to a simple floor of $2500.

Yet the range of compensation that victims of data breaches have gained from settlements of their claims are tiny compared to these arbitrary statutory damages. For instance, in the Home Depot breach, in which the email or credit card information of 50 million customers was compromised, the cash made available to Home Depot customers averaged $2.60[15]. In the infamous Ashley Madison breach, highly embarrassing information on 36 million customers was hacked and published. The settlement included about 20 cents on average for the affected customers[16]. It is difficult to describe these privacy actions as anything other than a vehicle for enriching the plaintiffs' lawyers[17], rather than compensating the plaintiffs for a loss.

Beyond the intangible privacy losses there are instances of actual harm from a data breach arising from post-breach identity theft. But the available data suggests these losses are both rare and bear little resemblance to either the statutory damages or settlement awards. In 2014 about seven per cent of U.S. residents over 16 —17.6 million people— were victims of identity theft[18]. Eighty-six per cent of these victims experienced the misuse of an existing credit card or bank account, where private and public insurance schemes significantly reduce the risk of economic loss. Four per cent of victims had their personal information activity stolen and used to open a new account or for other fraudulent activity. Thus, only about 14 per cent of identity theft victims (about one per cent of US residents over 16) experienced an out-of-pocket loss of $1 or more. Of the group experiencing financial loss, half suffered losses of less than $100 and 14 per cent lost $1000 or more.

It is unclear at this point how data subjects will fare in being made whole after a breach under the GDPR. In addition to a system of potentially very substantial administrative fines

[11] 15 U.S.C. §1681n(a)(1)(A).

[12] 18 U.S.C. § 2724.

[13] 18 U.S.C. § 2710(c)(2)(A).

[14] 47 U.S.C. § 551(f)(2)(A).

[15] 'Settlement Agreement and Release', In re: The Home Depot, Inc., Customer Data Security Breach Litigation, Case No. 1:14-md-02583-TWT (N.D. Ga.) at 22 (setting up $13 million settlement fund) (March 7, 2016).

[16] 'Stipulation of Settlement', In re: Ashley Madison Customer Data Security Breach Litigation, No. 15-md- 02669 (E.D. Mo.) at §§ 3.1 (gross settlement fund), 3.2 (less fund administration fees), 11.1 (less attorney's fees) (July 14, 2017). Actual settlement amounts will undoubtedly be higher, because the erstwhile customers will have affirmatively to make a claim for relief, and it is likely that only a single-digit percentage will seek compensation.

[17] Home Depot waived any objection to attorney's fees of up to $8.475 million. Settlement Agreement and Release at ¶ 61. In the Ashley Madison case the parties agreed to $3.7 million in attorney's fees. Stipulation of Settlement at ¶ 11.1.

[18] Victims of Identity Theft, 2014, Bureau of Justice Statistics, U.S. Dep't of Justice, (Sept. 2015).

for violations under Article 83[19], the GDPR states that '(a)ny person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered.'[20] And the GDPR certainly seems to suggest a robust theory of compensation, which should be 'full and effective' and where the 'concept of damage should be broadly interpreted.'[21] Yet if the actual out-of-pocket experience in the EU mirrors that in the United States, awards for actual damages should be small, while awards for dignitary harms perhaps will be greater, given the fundamental nature of the right infringed in the EU.

The relationship between the privacy-based damages system and actual losses seems distant at best. For nearly all victims of identity theft the statutory damages amounts are significantly greater than out-of-pocket losses. At the same time, the amounts awarded on average through tort litigation settlements are too small to be considered an award at all. This system fails to match compensation with loss.

The obvious flip side of this misalignment of loss with damages is the failure of the privacy system to provide data holders with accurate market signals to calculate how much they should invest in cybersecurity. Foreseeable liabilities should drive at least a minimum level of spending to prevent the liability. The privacy model fails here as well, in two regards.

First, the absence of any apparent relation between loss and damages gives the data holder no clue to how to trade cybersecurity investment for potential litigation loss.

Second, there is no obvious standard of care a data holder needs to achieve. The GDPR's treatment of privacy failures that arise from breaches offers few clues as to the level of care a data collector or processor must meet. The GDPR is expansive (and aggressive) on the issue of breach notification but the language on steps collectors and processors must take to prevent a data breach is short and uninformative:

> Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk…[22]

[19] Art. 83.4 permits 'administrative fines up to 10,000,000 EUR, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher' for 'infringements' of Article 32, governing the 'security of processing'.

[20] GDPR Art. 82.1.

[21] Id. at (146).

[22] GDPR at Art. 32 § 1 (emphasis added).

What is 'appropriate'? The only indication is a specific mention of 'pseudonymisation and encryption of personal data.'[23] Beyond that, the controller and processor simply are reminded of the obvious point that they should take account 'in particular of the risks that are presented ... from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.'[24] Perhaps the 'adherence to an approved code of conduct ... or an approved certification mechanism' may act as a mitigating factor, at least in the context of administrative fines.[25]

In the United States we substitute 'appropriate' with 'reasonable.' The FTC believes that a failure to maintain 'reasonable' cybersecurity is an 'unfair' practice forbidden by the FTC Act.[26] What is 'reasonable'? The FTC has never issued a regulation about 'reasonableness.' Instead it has bundled together 'ten lessons' from 50 settlements of actions it has brought for 'unreasonable' cybersecurity practices.[27] Because most of these cases involve companies making a number of 'basic, fundamental security missteps,' they are good descriptions of how a mass of obvious mistakes can amount to 'unreasonable' cybersecurity in particular circumstances, but provide little insight into what 'reasonable' cybersecurity might be in other situations.

A host of federal agencies also adopted a reasonableness standard in response to the Graham-Leach-Bliley Act's requirement that they 'establish appropriate standards for the financial institutions subject to their jurisdiction relating to administrative, technical, and physical safeguards' for customer information.[28] And to the extent a data holder is involved in a negligence action[29] arising from a breach, the standard is one of reasonable care. How is business supposed to make a calculated investment in cybersecurity given these amorphous standards in an environment where cyber risks are constantly in flux?

[23] Id. at § 1.a.

[24] Id. at §2.

[25] Id. at §3. Art. 83.2 requires that '(w)hen deciding whether to impose an administrative fine and deciding on the amount of the administrative fine . . . due regard shall be given' to a list of 11 aggravating and mitigating factors. Id. at (a)-(k). Among the latter is whether the defendant adhered 'to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42.' Id. at (j). Interestingly, Art. 82 contains no list of factors to govern the award of private damages.

[26] 15 U.S.C. § 45a.

27 Start With Security, A Guide for Business, Lessons Learned from FTC Cases at 1 (June 2015).

[28] 5 U.S.C. § 6801(b). See, eg: 16 C.F.R. § 314.3 (safeguards shall be 'reasonably designed' to achieve the objective of the Act). The various 'safeguard' rules are enforceable only by the relevant agencies. 15 U.S.C. § 6805.

[29] The inevitability of a negligence action reinforces the ill fit of the privacy torts to thinking about cybersecurity. The US privacy torts are intentional torts so the plaintiff has no need to show that the defendant failed to meet a standard to care. But the privacy torts do require the plaintiff to prove that the defendant's failure to protect her information was intentional, which is seldom the cyber-breach fact pattern. Seta v. Ready Rock Inc., 100 Ohio App. 3d 731, 740 (1995) (publication of private facts tort requires plaintiff to show that publication was 'made intentionally, not negligently.').

These concerns about the problems with using privacy protection as a legal framework for cybersecurity regulation of course beg for an alternative. On current course and speed, over a number of years we may perhaps see the courts hammer out a workable standard of care. But time is not on the side of the good guys in the cybersecurity fight.

A better approach would be to deal with the personal choice, damage calculation and cyber-investment problem more directly. For instance, one could imagine a scheme where various types of personal information are deemed to have monetary values once they are in the hands of data holders, coupled with an administrative strict-liability standard. This approach would have a number of salutary effects.

First, if personal data had some value there is at least a chance that data subjects would take greater interest in the circumstances under which they provide their data to holders, either directly as part of a transaction or by voluntarily sharing it.[30] Data values ought to vary from near zero for a credit card number (because the data subject frequently is held harmless after a loss of this data) to some significantly greater amount for data that can be used to steal an identity and fraudulently open new credit accounts which increases the chance of significant monetary losses to the data subject.

Second, data holders could be required to account for the contingent loss that the data they possess represents. Given the probability of an eventual breach of even the best-defended network, the Securities and Exchange Commission could require businesses to assess and put up a reserve for the contingent loss under the Financial Accounting Standards Board's Accounting Standard 450. This would lead data holders to treat held data as the liability it really is and take steps to reduce that liability by shedding personal data (or not collecting it in the first place). It would also give companies a number against which to candle their cybersecurity investments.

Finally, a strict liability regime would eliminate the randomness of 'privacy' recoveries, whether based on negligence or statutory regimes. Recovery is based on the designated value of the data lost, not on 'unmeasurable' privacy harm. And the societal cost of litigation that generally fails to provide meaningful relief to data subjects is eliminated.

[30] In order to keep the incentives in the right place, the data will have to value in circumstances in addition to the loss scenario. If the data were valuable only after a loss, some data subjects (who prefer money to privacy) would have an incentive to do business with a poor data holder in the hope of a breach.

Discussion: Cyber Security: Public Responsibility and Fundamental Rights, or Shared Responsibility and Regulatory Challenge?

MARIE-CHRISTINE DÄHN

The first session's first block concentrated on the question of whether cyber security should be viewed as an issue of fundamental rights and public responsibility or one of shared responsibility, both constituting a regulatory challenge for legislators in the EU and the U.S.. With a focus also on aspects like the impact of the General Data Protection Regulation (GDPR) on companies transferring and processing personal data across the Atlantic, the subsequent discussion shed light on the diverse facets of the topic. The input presentations followed the keynote given by Michael Weidner on "Cyber Security and Data Protection – Friends or Foes?" (not in this volume) and were provided by Théodore Christakis and Randy Milch.

Across different positions, it became clear that it is important to analyse whether a proactive or reactive legal approach would be more reasonable in dealing with cyber security in the first place. Reactive law adopts an ex post view on issues, on incidents that have already taken place and methods that have already been used. For instance, law enforcement activities are carried out after an incident has happened. On the other hand, proactive approaches are based on an anticipation of future problems and incidents that may arise. Instead of building on the analysis of past failures, it concentrates on how to avoid or regulate certain problems and crimes before they happen; measures to prevent crimes serve here as an example. As both approaches point in different directions, the question has arisen of whether they are fundamentally incompatible or could be combined in order to better address cyber security issues. While a reactive approach is an important component in deciding what legal measures to take, the participants remarked that it should be balanced by a proactive concept. Some measures, when employing both approaches, might make applying one or both concepts harder but they are not fundamentally incompatible. In the long term, the situation will be much better than it is today, since there will be more experience with the issues at hand as well as with the handling of the need for balance. The outlook for the proactive approach, however, remains uncertain at this point in time.

From a practical-technical perspective, it has been noted that the existence of a vulnerability does not always imply a risk. It often depends on the perspective of an organisation or person as well as of their particular interests whether an instance is perceived as a risk. In addition, not every risk which exists will be exploited, but that does not mean that affected or involved parties or legislators should be indifferent about it.

Following this debate on the general issues of cyber security and balancing proactive and reactive approaches, the discussion shifted to the new European data protection framework —the GDPR. While some participants characterised the U.S. and the European approach as still deficient with respect to the protection of individuals, others pointed out the improvements. With the GDPR, for instance, the notoriously patchy legal framework of Directive 95/46/EC 'on the protection of individuals with regard to the processing of personal data and on the free movement of such data' of 1995 becomes more harmonised; this was the main motivation behind choosing a regulation instead of a directive. Furthermore, a directive has to be transposed into the national laws of the Member States of the EU in order to become operational; a regulation, in turn, is directly applicable throughout the EU. Still, with the many flexibility clauses it contains, e.g. in the area of extensive employee data protection, the GDPR allows for a diversity of special rules in the Member States.

Besides this, one major focal point of the discussion has been the impact of the new European rules on companies. The regulation contains new instruments to regulate the processing of personal data, including new security measures to be taken by companies. An outstanding example is the Binding Corporate Rules (BCRs), originally developed by the European Union Article 29 Working Party and codified in Art. 47 of the GDPR. BRCs can be applied if a competent supervisory authority approves them and if such rules are in accordance with the consistency mechanism specified in Art. 63 GDPR. A common remark in the debate was that such instruments are widely overlooked in the debates. Regarding the improvements brought about by the regulation, it was strongly debated whether it introduces stricter requirements and makes enforcement easier. There has been no doubt, however, that the data protection authorities (DPAs) will try to increase the pressure on companies to comply, for instance by interpreting rules strictly. However, the participants were divided on the scale of the fines which could be imposed on non-compliant companies. The four percent clause in particular might not take the widely varying sizes of companies into account as much as it should. More generally, the criticism has been voiced that, when a problem arises, small companies find themselves confronted with other and potentially more difficulties than larger companies. The discussants observed that the GDPR fails to address the problems of small companies properly. Small and larger companies alike nevertheless have to adhere to the standards that the GDPR establishes —this applies equally to companies based both within the EU and without, if they provide services in the Union. Regarding the flow of data between the EU and third countries, companies insist that they own the generated data, although most of them cannot tell how much data they transfer between Europe and the U.S., for example. Some companies, moreover, have stated after the establishment of the Privacy Shield that they do not have such extensive data streams at all. The fact that from an economist's perspective the data should be where the companies need them points to one of the major conflicts of interest in this field, since both the data subjects and the regulators strongly oppose this view. Therefore, this issue requires further discussion.

On the aspect of the EU–U.S. relationship, the discussion repeatedly returned to the conference's main question, namely, the question of whether the approaches and frameworks of the U.S. and the EU could be combined at all as there are so many fundamental differences. Comparing both approaches, however, many participants pointed to the strong similarities that exist in the conceptualisation and regulation of privacy and data protection. A classic example is, for instance, the fact that both privacy and data protection are widely seen on both sides of the Atlantic as a means of constraining state power. Data protection and privacy nevertheless cannot be limited to restricting state practices, and neither in the U.S. nor in Europe have they been limited to regulating only state informational practices. Still, this is only one component. The European perspective further underlines the need for restrictions on the data-gathering and processing practices of companies since these are not always in accord with European data privacy and protection standards. Moreover, what both sides share are the challenges resulting from the technological developments which are affecting numerous aspects of social life; not only through everyday and personal usage but also due to the fact that they are increasingly becoming an essential part of the economy. And as past experiences in the EU as well as in the U.S. show, such technological developments have often brought about further advances in privacy and data protection legislation. The extensive processing of personal data in particular is considered problematic, mirroring the European perspective, even though some participants highlighted its economic potential. However, the U.S. and EU legal approaches admittedly differ on a more general level. Europe, on the one hand, pursues an omnibus law approach and treats state and private actors largely on an equal basis with respect to requirements for data processing. On the other hand, the U.S. establishes a sector-specific approach with a focus on self-regulation regarding data processing, with some oversight by the FTC. The highly controversial debate on these aspects showed that there is still a great need for discussion to find common solutions to common challenges.

Law Enforcement, Intelligence and Jurisdiction: An Intervention from a Business Perspective

GAIL KENT

Given all of the issues that we've talked about in here today, there are a lot of interesting conflicts. I spent 20 years in law enforcement, and some time in academia as well, trying to look at these issues; and what I thought I could usefully do, is to pull together some of themes that I'm seeing from the very privileged position of looking at what is happening around the world. I would echo a lot of what previous speakers have said about the EU and the US, leading the way for debate about cyber security on a road to be able to address privacy and data protection.

So, I start with the three trends I'm seeing, and I'm going to be —very hopefully— pragmatic and less theoretical, and talk about these three trends I'm dealing with every day around the world.

The first trend is that we have more data available than ever before. I try to take myself regularly back to what it was like when I first started as a law enforcement officer in late 1999, and I certainly didn't have the ability to know what my targets looked like, or know very quickly what they looked like. Now it is possible to identify what a target of law enforcement or intelligence investigation looks like. There is digital evidence on virtually every investigation. So, it's not just about cyber security, it's also about investigations into crimes that take place online, like cyber bullying or frauds or any sort of the abuse that you might see that is digital evidence there. It's also digital evidence when it comes to crimes that exist completely offline. So whether that's drug trafficking or money laundering because people are either using the internet to arrange their crimes or they have a digital presence, and that is very, very useful if you are an investigator. But what that means, is there are also more and more requests for data coming to companies like ours and you see countries around the world, trying to adapt for that. In terms of access to data for law enforcement, you see the UK, Hungary, Poland or Ireland having discussions about their access request for law enforcement, but you also see Spain at the moment, talking about what can it do to try and make sure it's matching its passenger name records to data that is on the internet, to people that are travelling, so try to even pre-empt investigations in terms of data. And then you also see, and I think very, very helpfully in the EU, you see a comprehensive discussion on e-evidence. I think it's definitely one of the ways the EU is leading the discussion. So, the first trend is there's more data, and law enforcement and governments want access to that.

The second trend, and again, it's one of these be touched upon a lot, is data breaches. We've seen greater concern about what data breaches mean. Data breaches have happened for certainly the 20 years that I've been involved in looking at cyber crime, but I think they're much more the high-profile and they're sort discussions that people have every day. They are not something that is only going to be on page 29 in the newspaper —it's going to be on the front page. And what we're seeing, and previous speakers have touched upon this, discussions about 'what does that mean' on a national level. And certainly in the States, you're not just seeing the federal government discussing what it means for data breach, you're also seeing every state in the United States come up with different iterations of what a data breach legislation should be like. And I think, we haven't quite got there in Europe, maybe the NIS Directive on the cyber security structure is going to take us to a much more holistic processing that would certainly be incredibly useful.

And a third trend that I'm seeing is a focus on national security and again that's really interesting. Not just for companies in governments but for individuals. So, what does terrorism mean, in terms of what companies should be doing, what should our response be to terrorism? That's something that we've seen to be debated nationally, and in a lot of member states, but we're also seeing it debated in across Europe and in other forums, like the European Union, G20, and the G7.

And if we look at the three trends —there's more data available, there are data breaches taking place that people are concerned about, there's national security issues that governments and individuals are concerned about— I think that Zach's four core themes are a really useful way because they all three areas are touching on all those four themes:

There is an interest in the intelligence agencies trying to handle data breach and a big interest in national security; you see law enforcement having the same interest; you also see a cyber security touch in all of those themes and you also see privacy. And I think that there are overlaps in all those different areas.

We've talked a lot about the intelligence agencies and law enforcement on the cyber security and privacy side. What we haven't maybe gone into in as much detail, is what does this complexity means in the areas like encryption and government hacking where you have got some conflicts but where we may have the ability to reconcile conflict and to reconcile in a way that there is trust.

One of the things I now want to move to, is the fact that to have any debate on these issues we really need to get into the really, really specifics and that's something that I think we're missing at the moment. In both the US and then Europe we're not discussing these issues in a way that looks at the facts and that's why it's great to have so many academics at the table.

So much in this discussion is based on what people perceive happens and what their perceptions of other countries are and what their perceptions of what the countries are doing vis-a-vis their own countries other than what is actually happening. There are often not many experts in the room there as there should be.

So, because of the lack of specifics and concrete facts, what we see is often unnecessary complexity, duplication and conflicts within and between individual countries. You mentioned the GDPR and the NIS Directive, and what will individual countries do to make sure that those are harmonized, so that you don't have regulation in France that goes against that in Ireland. Who is it, when do we report, who do we report to and what do we report? And if you can imagine that that's a big issue for Facebook with the resources that we've got and trying to work that out, what's it look like for a smaller company that is trying to look through that? So, we see conflicts within countries, we also see conflicts between countries, and the most obvious ones, that I'm dealing with my day-to-day basis, is about access to data in the US, compared to access the data in the EU. So, US law forbids US companies from providing content unless US legal process as follows under the Electronic Communications Privacy Act. That puts EU and other law enforcement in a really difficult position: how do we deal with these conflicts of law, and I'm sure, you're going to talk more about conflicts of law and more than that means for global companies in terms of deciding which law we follow.

Then we also see, jurisdiction of one country versus an international perspective, and this is where I think that there's a requirement for a real single market debate. This is particularity interesting because I think in theory, every member state would like to be attached to the digital single market, as long as the digital single market is mainly established in their own jurisdiction! And you see that also in the debates over the GDPR and the NIS Directive, in terms of who has the ability to investigate and has jurisdiction over companies. I think that's one thing we'll increasingly keep debating, but if we can come up with some sort of response, that would be fantastic.

And then one last conflict that I see every day in individual jurisdictions, is security versus transparency. So, there is a push for more transparency and I hope that we as a company are also following as well to be increasingly transparent, but at the same time, if you're looking at the discussion in national security and law enforcement investigation, there is a pressure for continuous secrecy. You see that again in the EU directive on combating terrorism[1] and the discussion about encryption, but unless you're in the room, it's very difficult to understand what is it exactly that the European Union is advocating to help law enforcement deal with the problems around that and encryption.

[1] Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA, in: OJ L 88, 31 March 2017, p. 6–21, at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32017L0541.

So, overall what does that mean that we as companies are trying to do, and what do we see, and what was our response? I think, the first thing to say is that we in no way think that we have all of the answers on this, and it's one of the reasons why it is so fantastic to be here, to be listening to the level of debate and this is why we do things like this because it's really important for us to be listening to your voice and perspectives and what I should be responding to.

At the moment, in addition to listening, I think we have two different drivers: one is a thing that is absolutely paramount to us, is what is the best thing that we can do for the safety of our users?

Facebook itself has 2 billion users —an incredible responsibility in terms of the data that we are stewards of. With WhatsApp we've got a billion users —a huge amount of responsibility for users that are already enrolled there, that are using our services for a huge variety of different purposes, from business to personal relationships in entirely different regions around the world.

What is the best thing that we can do for the safety of our users? (I had a discussion with a German colleague recently, and it's interesting in Germany that in German there's no difference between security and safety. So, what does that actually mean for how you deal with something that has to do with security issues which are traditionally seen as, I think, more important for government compared to safety which is maybe the more of a person's own responsibility, and does that have an impact?)

Safety and security has to be a user-based approach. I would respectfully disagree with anyone saying that the user has responsibility because what we found is that responsibility can be confusing for some users. Technology changes so quickly, and I genuinely have spent a lot of time trying to think about how do we get people to take the same responsibility for their online safety and security as they do for their physical safety and security and we're not yet there. So, we are at the position that we are starting from trying to make it as easy as possible for people to know that their data is safe and that they are safe on Facebook.

Our second driver is: our responsibility to contribute to both the cyber security ecosystem and also that general security ecosystem. What can we do in terms of open-sourcing our cyber security products? What can we do in terms of sharing our knowledge of what a user-based approach means, but also, what can we do in terms of helping government understand the conflict that we are experiencing? Are some of the solutions equipped to resolving those conflicts? So, what can we do in terms of like working with the Irish government, to explain from our perspective? Where do the GDPR and the NIS Directive demand action from us and what are the complexities that we offered? And, similarly, what can we do with the European Union to help them work towards better access to law enforcement, for investigations in a way that doesn't increase conflict between laws but reduces them?

In conclusion, I thought I'd end up with some of the questions that we are still collectively thinking about. Some of these are pointing to what Paul Nemitz said at the start, what is it that allows us to offer the best service for our users that takes into account the safety? What are the obligations that we should be doing, what are the best frameworks? And then too, I think, what is it that we can do to develop trust? It's a thing in this area, so I said it's based on perceptions and ideas rather than actual facts, what can we do to try and build up that trust?

We should have discussion based on facts; this is also developing trust. It's also the currency that Facebook and the other tech companies are absolutely required to offer in the services that we do.

One final comment: these are incredibly complicated and huge subject areas and I think just in the discussion that we had in the first two hours we covered vast quantities of issues. What can we do to try to break these down into very, very practical discussions that will help develop trust and come up with some of the solutions to these areas, rather than continuing what can often be too long and open-ended conversation where the solutions lie very, very far away?

Better intelligence oversight through technology? New perspectives on an old problem.

THORSTEN WETZLING

INTRODUCTION

Modern security and intelligence services use a range of digital powers to pursue their important mandates. Some of these powers, such as the electronic surveillance of communication data or computer network exploitations, can be highly invasive and may substantially interfere with human rights. Effective checks and balances are therefore imperative in order to review the legality and propriety of the use of such powers. Independent review bodies have to be able to challenge and, where necessary, penalise their abuse.

Despite recent reforms to further professionalise national intelligence oversight frameworks in Europe and North America, effective intelligence oversight remains an ambitious, unattained and vague benchmark on both sides of the Atlantic. Oversight dynamics on the ground continue to be marred by a range of problems, including ineffective control mechanisms, regulatory capture, a lack of technological knowledge and insufficient motivation to engage persistently in proactive and unglamorous investigative review work. In addition, one can point to no-go-zones and accountability gaps in conjunction with international intelligence cooperation and the outsourcing of intelligence functions to private contractors.

It is against this backdrop that the search for oversight innovation remains important. It should not be driven by government and legislators alone. Considering how the pace of technological innovation challenges core concepts of intelligence law and oversight practice, a broader set of perspectives is now needed to identify and promote viable options for positive change.

Drawing on insights from an ongoing transatlantic project,[1] this text first elaborates on a few current challenges to illustrate the need for oversight innovation. Next, it points to aspects where a more systematic and creative use of technology might help oversight bodies to better address known deficits. It then sketches out a few options that may make a difference if put into practice. Whether and how this might work and whether it might encounter new problems requires further analysis and actual feedback from intelligence governance practitioners across different branches of government. This dialogue can

[1] For more information on the project, see https://www.stiftung-nv.de/en/project/international-cyber-security-policy#drei.

obviously not be taken for granted and requires a carefully calibrated strategy of its own.[2] Only with sufficient support from oversight practitioners can any of the ideas be turned into a viable technology-driven reform agenda.

ON THE NEED FOR OVERSIGHT INNOVATION AND A PATH TOWARDS IT

As the conference title rightly conveys, significant differences exist in both Europe and the U.S. as regards privacy and cybersecurity on the books and on the ground. This is certainly true also in the field of intelligence governance. There is no shortage of guiding principles and international calls for effective democratic control and independent oversight. For a recent example, consider the UN resolution on the right to privacy in the digital age: It 'calls upon all States to establish or maintain existing independent, effective, adequately resourced and impartial judicial, administrative and/or parliamentary domestic oversight mechanisms capable of ensuring transparency, as appropriate, and accountability for State surveillance of communications, their interception and the collection of personal data'.[3] While it is important to regularly and visibly remind governments of the need to allow independent review of their invasive surveillance practices, the UN's call for independent, competent, informed, agile and resourceful oversight bodies has remained relatively inconclusive and as such is very convenient for Member States to support. By contrast, it is a much harder task to establish robust oversight in actual practice and to agree internationally on best practices. Recently, the international community rebuffed the UN Special Rapporteur on the Right to Privacy's attempt to establish international standards on government surveillance and human rights safeguards.[4]

Seeing intelligence oversight thus as an ambitious, unattained and vague benchmark, the transatlantic project mentioned above considers oversight innovation as work in progress not just for legislators and government. It seeks to bring multistakeholder expertise together in an attempt to develop pragmatic and innovative solutions to current oversight challenges. This includes regular transatlantic workshops with former oversight body representatives, telecommunication providers, academics and civil society representatives. Using collaborative work methods in carefully scripted workshops, it offers a chance to better understand the underlying factors for good or bad practices and the potential for oversight innovation, regardless of the constitutional and political differences among countries.

[2] One such strategy, for example, is the European Intelligence Oversight Network. More information available at https://www.stiftung-nv.de/sites/default/files/eion_project_strategy_brief_0.pdf.

[3] http://www.un.org/ga/search/view_doc.asp?symbol=A/C.3/71/L.39/Rev.1.

[4] See https://www.ip-watch.org/2018/03/07/un-rapporteur-privacy-rebuffed-surveillance-oversight-negotiations/.

As a first step, the project identified examples of post-reform oversight deficits in Europe and in the U.S. Next, the workshop participants clustered and weighed a wide range of challenges according to different parameters such as criticality. Among those challenges were secrecy and the flaccidity of some oversight members. While these are critical and unresolved aspects, the group then focused on challenges that concern access to information. More specifically, the question arose of how technology might be used to allow for a less credulous and more adversarial oversight game in the future.

CURRENT AND FUTURE CHALLENGES

In December 2016, the Bundestag passed the most comprehensive reform of intelligence legislation in over two decades. Yet many known deficits have remained in place.[5] For example, at present, there is hardly room, let alone sufficient resources for a rigorous monitoring of data processing through the quasi-judicial G10-Commission. Moreover, there is hardly any digital documentation that would allow individual members of the G10-Commission to review the way in which their authorisation decisions have been implemented.

By European comparison, both the Netherlands and the United Kingdom have experienced granular debates about the standards in law and in practice concerning the authorisation of bulk surveillance. Irrespective of what one makes of the authorisation standards that these countries have adopted, the equally —if not more— important safeguards concerning data handling by intelligence services remain insufficiently legislated across Europe.[6] How the services treat data once they have acquired it and whether their data minimisation and data deletion procedures are adequate and independently verified is a matter that requires further attention and scrutiny.

Another challenge lies in what may be called 'non-intelligence intelligence'. This includes the re-use of commercial databases for intelligence purposes. More generally, as more and more software seems to be converging across different sectors, it becomes more difficult to distinguish clearly between data-sensitive intelligence and police and military operations. By contrast, the remit of intelligence oversight bodies remains strictly tied to intelligence service activity. It is time to ask more critically what it is that oversight bodies should be reviewing and whether some of the distinctions used in national security legislation and parliament are outdated.

[5] For a more detailed analysis of the reform, see: T. Wetzling, Germany's intelligence reform: More surveillance, modest restraints and inefficient controls (Berlin: Stiftung Neue Verantwortung, 2017). Available online: https://www.stiftung-nv.de/de/publikation/germanys-intelligence-reform.

[6] For a recent review, see Q. Eijkman, N. van Eijk and R. van Schaik, 'Dutch National Security Reform Under Review: Sufficient Checks and Balances in the Intelligence and Security Services Act 2017?' (2018). Available online: https://www.ivir.nl/publicaties/download/Wiv_2017.pdf.

Another challenge has to do with the fact that counter-terrorism and cyber security accrue different data needs. In 2015, the Bundestag added a clause to a central intelligence law that allowed non-targeted bulk surveillance to prevent hostile cyber operations against critical infrastructures. While counter-terrorism intelligence data needs were often portrayed as being kept within limits, it appears that the vigilant protection against cyber threats requires a different monitoring of electronic signals. How an individual oversight body can ensure that the interception of communications data is proportionate, given such different data needs, and how it can identify abuse has not become easier to understand.

Another aspect that can be raised to highlight current oversight problems is the insufficient regard for the summary effect of existing surveillance activities when authorising new warrants. In 2005, the German Constitutional Court coined the term 'Überwachungsgesamtrechnung'. Basically, the Court announced that individual authorisation decisions rarely take into account the total sum of existing surveillance measures. It would indeed be beneficial to future intelligence governance if the authorisation of warrants had to be made in full cognisance of other active measures. This idea has not resonated enough among security circles. At the time that the G10 Commission or the FISA Court is being asked to authorise an individual surveillance warrant, do they arrive at that decision with sufficient knowledge of other existing surveillance measures that are being run for the same purpose? At present, the reviewers will only assess the merits of a warrant on an individual basis. Here it might be possible to visualise some form of surveillance warrant that would in future help overseers to determine the need for more surveillance.

POTENTIAL TECHNOLOGICAL SOLUTIONS?

These are only some of the challenges that have come up in the ongoing project work.[7] As concerns potential legislative or technological solutions to better address some of these challenges, we have begun to search for ways in which judicial overseers can be empowered with readily accessible information on the totality of existing surveillance measures at the time when they are deciding whether or not to authorise new warrants. Here one needs also to discuss whether this should only concern the information on existing measures by national security services or whether the growing density of existing European counter-terrorism databases can also be added to a potential visualisation tool.[8]

[7] For a more comprehensive overview, see: T. Wetzling, Options for more effective intelligence oversight. (Berlin: Stiftung Neue Verantwortung, 2017).

[8] H. Busch and M. Monroy, 'Counter-terrorism and the inflation of EU databases' (2017). Available online at https://digit.site36.net/2017/05/23/counter-terrorism-and-the-inflation-of-eu-databases/.

Another idea by a group member was to establish authorised third-party time-stamping services for warrants and the publication of cryptographic fingerprints for such information. This would address some of the current deficits in the ex-post control of individual surveillance measures because it would allow reviewers to link the activities to an existing warrant and see whether the activities have been compliant with the warrant or not. Any deviation of data acquisition (e.g. a different telecommunication net or a longer duration) could thus be detected without revealing critical information.

Another idea that has come up is to find a way to better quantify intrusion. We need new instruments to unpack and evaluate the privacy intrusion of data processing tools. The majority of laws regulating the use of SIGINT techniques are predicated on a two-stage authorisation framework —an initial sign-off for large-scale access, and a second authorisation process when an intelligence officer wishes to view or analyse the collected information (usually only required if viewing a particular citizen's material). This authorisation model often fails to take into account interference with rights in between these two stages caused by the use of data processing and analytical techniques. These include the use of speaker recognition, emotion detection, language identification, content summarisation, link analysis as well as automatic enrichment of material, and the processing of material creating query-focused datasets. As these techniques become more widespread, a common understanding of how and where privacy intrusion occurs and is impacted will be essential to ensure that a rights-compliant and appropriate framework exists (both in internal agency policy and in statute). Opportunities to attempt to quantify this intrusion could also provide critical data to overseers, and methods to model various intrusion points could help provide some means of measuring exactly to what extent an individual privacy is being interfered with.

Another way forward would be the installation and independent certification of oversight interfaces. There are backend interfaces for the law enforcement community, but there is no such direct access for oversight bodies. Some European countries such as Norway or the Netherlands have given independent oversight bodies almost exclusive access to the online directories of intelligence service databases. One could think about requiring manufacturers to build in standardised, independently controlled interfaces at interception point (i.e. at an internet hub such as the Frankfurt-based DE-CIX) to better comprehend the acquisition practice of the intelligence services and to evaluate the practical necessity of the enormous amount of data held.

Also, as regards the data minimisation process, some countries have publicly revealed their elaborate filter systems that are being put in place to adhere to different data protection standards for national and non-national data. Provided an independent verification of the filtering process could be achieved, one could run so-called 'sock puppet audits' on the system. It would allow the review body to test the performance of the filtering process by entering false data into the system and see if the filters were

able to identify such an irregularity. This ties in with questions regarding the design, performance and transparency of control algorithms.

CONCLUSION

What can make the threat of defunct intelligence oversight loom less large? To alleviate existing capacity problems, it is time to think more creatively about how technology can be designed and deployed to better serve the overseers' needs. As intelligence and security services are pioneering digital tools for their work, it might seem as too obvious a solution to also apply advanced technological tools from the overseers' end. However, this is at present generally not happening, even though some oversight bodies might be currently experimenting with different types of solution.[9] More research and open dialogues are clearly necessary so that viable technological solutions can be identified and combined with better training of the overseers in combination with properly staffed and robust secretariats with legal, political and technical expertise.

[9] K. Otter Olsen, 'De hemmelige tjenestenes tekniske kapasiteter – kontrollutfordringer' (Annual EOS-conference, Oslo, 5 April 2017). See also M. R. Koot, 'Dutch Review Committee on the Intelligence & Security Services (CTIVD) to (self-)assess effectiveness of lawfulness oversight re: large-scale & data-intensive spying' (2017). Available online at https://blog.cyberwar.nl/2017/04/dutch-review-committee-on-the-intelligence-security-services-ctivd-to-self-assess-effectiveness-of-lawfulness-oversight-re-large-scale-data-intensive-a/.

Discussion: Law Enforcement, Intelligence and Jurisdiction: Approaches and Conflicting Interests in a Transatlantic Perspective

MARIE-CHRISTINE DÄHN

The second block of the conference's first session aimed at analysing regulatory approaches as well as conflicting interests in the area of law enforcement, intelligence, and jurisdiction from a transatlantic perspective. Gail Kent, Thorsten Wetzling, and Mark Lange provided the initial input presentations. The most important aspects dealt with in the subsequent discussion were the localisation of data, the movement of data, and the role fundamental rights play from a legal perspective. Furthermore, practical problems of law enforcement and the influence of court rulings were debated.

The first issue discussed was the normative implication of data localisation as a defense against security and privacy threats. Data localisation is a policy or regulatory approach that requires that citizens' data should be processed within the national borders of a country. This could, as critics emphasised, lead to a so-called 'balkanisation of the internet'. However, the participants remarked that localisation comes at a cost, while it is unclear what these costs are in general and, more specifically, what costs companies have to bear in order to stay in the market when data localisation is applied. China served as an example of a country where data is systematically localised: the servers there are basically inaccessible from other countries. Shifting the focus to the EU, one participant argued that companies can indeed still move data around in Europe, so data is not generally kept exclusively within national borders. In contrast, there are many attempts to localise data by states around the globe. In the case of Europe in particular, it has to be kept in mind, as a discussant remarked, that Europe only engages in conditional data localisation since it merely demands a similar level of data protection at the target location. By extension, it remains disputed whether the GDPR constitutes a case of data localisation.

Returning to the original question, the participants weighed the pros and cons of data localisation. One primarily technical advantage that has been highlighted is the reduced latency if a local data centre is established. Moreover, the data stored and processed locally can potentially be better controlled and secured. Contrary to this, the objection has been raised that data stored locally is not necessarily more secure as cyber security and data protection dangers and risks are often global in nature, and cyber attacks can be directed at national servers as well. At the same time, concerns are also raised about the possible surveillance of users. For companies, a major problem emerging from data localisation is that it might hinder foreign investment and create barriers because opera-

tions could become more complicated and costly. An important aspect —often neglected in the debates but emphasised by one participant— is that data is not just a tradeable commodity; it concerns the lives of people. Hence, this discussant added that data should always travel with protection, whether it is within a state or across borders.

Later, the focus of the debate shifted towards privacy. One participant particularly emphasised the more basic distinction between privacy as a subjective fundamental right and privacy as an objective value. This aspect has been discussed mainly with regard to law enforcement and intelligence agencies. It has been noted that the different understandings of privacy also reflect different understandings of the harm posed by surveillance or the use of data in criminal investigations. Consequently, some discussants highlighted the fact that there will not be a general solution to all the pressing problems attached to the divergent positions, but that specific solutions for specific problems can and will be found. Criticism has been raised, however, regarding the overall focus of the law enforcement debate. The participants remarked that there is a bias in the European viewpoint towards the British and German perspective and that more time should be taken to take a closer look at, for instance, Hungarian, Polish, or Spanish experiences and cases. A European discourse has to include the positions and interests of actors in all countries of the Union. Such different approaches with respect to distinct EU Member States can also be recognised in the case law of European courts. In this regard, one participant provided the example of the European Court of Human Rights (ECtHR), which has repeatedly ruled that Eastern European countries' surveillance laws impinge on the right to privacy (European Convention on Human Rights Art. 8), while some Western European countries' surveillance laws have just recently reached the court.[1] Across these differences, the participants outlined that it is important to determine how regulation on protection and rights could be formulated in a manner that every European Member State and its citizens know what their rights actually are.

[1] One possible reason for this dissimilar development might be that constitutional courts in Western European countries often solve cases at the national level and that their rulings are perceived to be more legitimate than in Eastern European Member States. The UK is an exception where complaints are also often brought before European courts. One example of legal complaints being solved at the national level before being referred to the European level is Germany. In 1984, on 20 June, a constitutional complaint reached the Federal Constitutional Court, which ruled that it is unjustified to restrain the confidentiality of mail and telecommunications by imposing surveillance measures for internal security purposes. This was continued with regard to the Federal Intelligence Service, in the Constitutional Court's ruling of July 14 1999. Here it was decided that while Art. 73 No. 1 of the Basic Law grants the Federal Intelligence Service the right to collect, utilise, and transmit telecommunications data, it is still bound in that by Art. 10 of the Basic Law, from which it follows that the use of such data is restricted to the purposes for which they were collected. Finally, on 27 February 2008, the Federal Constitutional Court ruled on the guarantee of confidentiality and integrity of information technology systems. In this regard, the Court stressed that the secret infiltration of an information technology system has to be restricted principally by judicial order. A law authorising such an intervention has to include provisions which protect the core areas of private life. In these three instances, a constitutional court ruled on surveillance issues at the national level and solved them without referring to the European courts. However, that does not mean that references to the ECtHR in such matters are excluded in the future.

As has been touched upon above, case law created by courts plays a key role in defining rights and jurisdictions. The current Microsoft and Google cases in particular received much attention from the discussants. The United States v. Microsoft Corp. case fell into the 2017-2018 term of the U.S. Supreme Court. On April 17 2018, the Court decided that the case be dismissed as moot since the new Clarifying Lawful Overseas Use of Data Act (CLOUD Act) had come into effect and the new warrant resulting from it replaced the old warrant of the Microsoft case. Nevertheless, the case raised important questions regarding the handling of data in law enforcement. Initially, Microsoft refused to disclose e-mails stored in an account in Ireland to U.S. law enforcement authorities in 2013. The legal foundations of this case, set up under Section 2703 of the Stored Communications Act, can be interpreted disparately. While the New York District Court ruled that this Act does not include territorial limitations of application, the United States Court of Appeals for the Second Circuit (case 14-2985) decided that there are limitations and that Microsoft was not bound to hand over e-mail data to the U.S. government which was exclusively stored on servers outside the U.S.. Regarding the location of the data, it has been argued that Microsoft migrated the data to their users' needs as indicated by their territory. Microsoft referred to the Mutual Legal Assistance Treaty (MLAT) between the U.S. and Ireland and argued that the U.S. government should turn to the Irish authorities with its request. MLATs are agreements between two or more countries specifying how to handle the exchange of evidence between them in an instance of law enforcement. The issue of transborder law enforcement access has become important not only in the present Microsoft case, but also in the Google case. In 2017, Google was ordered by a U.S. judge to hand over e-mail data to the U.S. authorities for legal investigation (In re: Search Warrant No. 16-960-M-01 to Google). Like Microsoft, Google refused to comply. Contrary to the Microsoft case, and despite the case also being filed under the Stored Communications Act, a U.S. judge in Philadelphia decided that Google had to comply with the FBI's search warrant. However, referring to press records, one participant added that Google intends to appeal the judgment, especially in the light of the Microsoft case. As can be seen from both cases, the actual location of data significantly influences which rules are applicable, while at the same time it shows the very contestedness of this issue and the need for further clarification and interpretation. One of the main questions remaining is when to classify data as extraterritorial and what follows from that. Nevertheless, at the end one participant reminded the conference that this is not solely a U.S. issue because, for example, the Investigative Powers Act of the United Kingdom, passed in 2016, gives its intelligence services wide-ranging surveillance powers —exactly like those which the U.S. agencies have tried to use in the Microsoft case. What becomes clear in this, however, is that the issues arising from this topic are not restricted to one country and have to be approached jointly in order to provide clarity.

LOOKING FOR COMMON GROUND IN A GLOBAL PERSPECTIVE

GDPR, Privacy Shield and the Framework Agreement: The EU Perspective

KAI VON LEWINSKI

PERSONAL DATA, COMMON GROUND, DIFFERENT VIEWS

The EU has established the common market (Article 3[3] TEU) and provides an area of freedom, security and justice (AFSJ; Article 3[2] TEU, Articles 67–89 TFEU) for its Member States and citizens. In this capacity, the EU has introduced a common data protection (law) standard within the Union. This was originally implemented by the Data Protection Directive 95/46/EC in 1998 and has been brought up to date by the General Data Protection Regulation (EU) 679/2016, which comes into effect in May 2018.

The U.S. legal system is based on the same Western values and has the same background as the European one, as it focuses on the individual (and not a group or society as a whole). Nevertheless, U.S. privacy legislation has a different approach towards the protection of personal data and privacy. This is usually put into a nutshell by the contrasting concepts of 'freedom' or 'liberty' on the U.S. side and 'dignity' on the EU side,[1] or by framing the U.S. approach as 'harm-based' and the European approach as 'rights-based'[2]. It can be said with a reasonable amount of simplification that U.S. privacy legislation is considered to be more favourable and less restrictive to data processors.

Such differing forms of regulation would be perfectly fine if they did not apply to data. It is the nature of data to flow. And since they flow around the world, data do not stay within the spatial scope of application of a certain legislation (here: the EU legislation). And, eventually, they may flow to the United States. This undermines the (effectiveness of) EU data protection and it puts EU data service providers and processors at a disadvantage compared to their U.S. competitors.

PRIVACY SHIELD ON THE BOOKS

The challenge, especially for the European Union, has been —and still is— to square the triangle of maintaining and enforcing EU data protection standards while not being able to persuade or force the U.S. to adopt standards of data protection which are adequate for Europeans and not blocking transatlantic data flow.

[1] J Whitman, 'The Two Western Cultures of Privacy —Dignity versus Liberty' (2004) 6 Yale Law Journal, 1153, 1161; see also, with an empirical approach, K Bamberger and D Mulligan, Privacy on the Ground: Driving Corporate Behavior in the United States and Europe, Cambridge, Massachusetts, MIT, 2015, and K Bamberger, 'Privacy on the Books and on the Ground' (2010) 63 Stan. L. Rev. 247.

[2] For an attempt to amalgamate the two concepts see R Poscher, 'The Right to Data Protection. A No-Right Thesis' in: R A Miller (ed), Privacy and Power, Cambridge, Cambridge University Press, 2017, 129, 133 et seq.

A whole set of instruments in European data protection law[3] addresses this issue: most important are consent (Article 49[1][1][a] GDPR), exceptions by law (Article 49[1][1][b–g] GDPR), and approval by data protection authorities (Article 49[3] GDPR). Special constellations are addressed by specific sets of rules, e.g. air travel by the PNR agreement[4] and banking by the SWIFT agreement.[5]

Because none of these instruments suits the vast streams of personal data flowing across the Atlantic, the 'Safe Harbour'[6] was introduced. It modified the general rule of EU data protection law that the exportation of personal data is not allowed if an adequate level of data protection is not guaranteed in the destination country (originally Articles 25, 26 DPD; today Articles 44–50 GDPR). Under the Safe Harbour regime, it was possible to export data to the United States if the data importer had signed up to the Safe Harbour principles. These principles consisted of material standards for the processing of personal data, data subjects' rights and enforcement procedures by U.S. authorities[7] (namely the FTC and the Transport Authority). The self-certification process, in particular, and a 'check the box' mentality towards the specified Safe Harbour principles[8] came in for heavy criticism.[9]

The Safe Harbour solution was legally challenged by the data protection activist Maximilian Schrems in his crusade against Facebook.[10] In a strict sense only for formal reasons, the ECJ declared Safe Harbour 'closed'.[11]

But soon 'Safe Harbour' was reopened under the new name of 'Privacy Shield'. The material standards and data subjects' rights have remained basically unchanged compared to Safe Harbour.[12] The main difference is that obligations on companies have been strengthened, a more robust enforcement as well as more safeguards with regard to U.S. government access to data have been provided, and more adequate mechanisms for dispute resolution have been established.[13]

[3] Cf. F Boehm, 'Assessing the New Instruments in EU-US Data Protection Law for Law Enforcement and Surveillance Purposes' (2016) 2 EDPL, 178–190.

[4] Cf. C Casagran, 'The Future EU PNR System: Will Passenger Data Be Protected?' (2015) 3 European Journal of Crime, Criminal Law and Criminal Justice, 241 et seq.

[5] Cf. V Pfisterer, 'The Second SWIFT Agreement Between the European Union and the United States of America —An Overview' (2010) 11 German Law Journal, 1173 et seq.

[6] European Commission Decision 2000/520/EC.

[7] See European Commission Decision 2000/520/EC, Annex I 'List of U.S. Statutory Bodies Recognized by the European Union'.

[8] See R Weber, 'Transborder data transfers: concepts, regulatory approaches and new regulatory initiatives' (2013) 2 IDPL, 117, 126.

[9] Summarised by D Greer, 'Safe Harbor —A Framework that Works' (2011) 3 IDPL 143, 145.

[10] Brief portrait in F.A.Z. [Frankfurter Allgemeine Zeitung], 26.01.2018, 8.

[11] ECJ, Case C-362/14; N Cohen, 'The Privacy Follies: A Look Back at the CJEU's Invalidation of the EU/US Safe Harbor Framework' (2015) 3 EDPL, 240 et seq.

[12] M Schrems, 'The Privacy Shield is a Soft Update of the Safe Harbor' (2016) 2 EDPL, 148 et seq.

[13] Cf. European Commission, Report from the Commission to the European Parliament and the Council on the first annual review of the functioning of the EU–U.S. Privacy Shield, COM(2017) 611 final, 2; in more detail see K Daugirdas and J D Mortenson, 'Contemporary Practice of the United States Relating to International Law' (2016) 4 American Journal of International Law, 347, 360–368.

PRIVACY SHIELD ON THE GROUND

On the ground —and despite the fact that they are doomed[14]— Safe Harbour and Privacy Shield seem to be success stories. Some 2,400 enterprises have participated in them[15], and the transatlantic data continue to flow and grow.

According to many experts, this success can be attributed to a lack of enforcement by the U.S. authorities. Investigations by U.S. authorities have been reported in no more than three cases,[16] and the numbers I have for Safe Harbour are something like 40 inquiries. Generally, their approach is described as being reactive, and not proactive.[17] And an independent ombudsperson, as another designated supervisory element of these schemes, has not even been appointed yet.[18]

Another loophole in the Privacy Shield is the exceptions for U.S. security agencies. To fight the 'War on Terror', U.S. intelligence and security forces have far-reaching rights to collect data under U.S. law. The U.S. constitution only protects U.S. citizens from data collection and surveillance, at least to a substantial extent.

PRIVACY SHIELD IN THE BIG PICTURE: ONE OF MANY INFORMATION LAW COLLISION REGIMES

The squaring of the triangle —bridging the discrepancy between EU standards and U.S. standards without substantially impairing transatlantic data transfer— is a collision of jurisdictions problem.[19] Collisions of legal systems cannot be avoided in an information and data context because data flow. Only a 'Great Firewall', like that erected around China, can prevent trans-border data flows and, consequently, data law collisions.

A rational solution requires a comprehensive analysis. An analytical grid in this context (inspired by Wolfgang Friedmann[20]) might include the following categories: maintaining sovereignty; co-ordination of the scope of application of the respective laws,

[14] Schrems II is on the way (submission decision of the Irish High Court, 4.10.2017; ECJ, 22.11.2017, T-670/16 (Digital Rights Ireland v. Commission), ECLI:EU:T:2017:838; ECJ, 21.06.2017, T-737/16 (La Quadrature du Net v. Commission) ECLI:EU:T:2017:453); ECJ, 25.01.2017 – C-498/16, ECLI:EU:C:2018:37.

[15] F.A.Z. (Frankfurter Allgemeine Zeitung), 26.09.2017, 24. The Safe Harbour scheme was reportedly used by over 3,200 enterprises.

[16] F.A.Z. 26.09.2017, 24.

[17] Loc cit, citing EU Commissioner Věra Jourová; cf. European Commission, Report from the Commission to the European Parliament and the Council on the first annual review of the functioning of the EU–U.S. Privacy Shield, COM(2017) 611 final, 5.

[18] Cf. European Commission, Report from the Commission to the European Parliament and the Council on the first annual review of the functioning of the EU–U.S. Privacy Shield, COM(2017) 611 final, 4 and 6, and Article 29 Working Party, 'First Annual Joint Review of the Privacy Shield' (press release of the November 2017 plenary meeting) of 05.12.2017, 1.

[19] K von Lewinski, 'Privacy Shield —Notdeich nach dem Pearl Harbor für die transatlantischen Datentransfers' (2016) 4 Europarecht, 405–406.

[20] W Friedmann, The Changing Structure of International Law, London, Stevens & Sons, 1964, 60–71. Friedmann proposes a three-level structure of international law: (1) international law of co-existence, (2) international law of co-operation, and (3) regional law of co-operation.

and harmonisation of legal systems. If we apply this analytical grid to the transatlantic data protection law regime of Privacy Shield, we can identify the following elements:

MAINTAINING SOVEREIGNTY

The primary level of international law, according to Friedmann and the first level of the analytical grid presented here, consists in the rules of mutual respect for national sovereignty.[21,22] And sovereignty has always been, and still is, a territorial concept. It is a result (and a function) of sovereignty to set and to maintain legal standards. In this capacity, EU legislation has established a certain level of data protection in the EU by the GDPR —or rather, from a U.S. perspective, the establishment of this concept of data protection as such.

Any regional or territorial approach to information law in general and to data protection in particular has to cope with the potential ubiquity of data and information. To fully and sovereignly apply its own regulations to data, a legal system has to fence in digital data in its own territory.

This is the approach in China with its aforementioned 'Great Firewall'. On a conceptual level, the adequacy requirements of the GDPR aim to achieve the same result as they block transmission of data by law. The difference to authoritarian regimes is, of course, that media content is not restricted and that only the outflow, not the inflow, of data is restricted.

CO-ORDINATION

The second level of an international collision of jurisdiction regime is co-ordination. Co-ordination is the classic instrument of collision of law. It addresses questions of reciprocal or unilateral (non-)acceptance of other countries' and other jurisdictions' standards.

Restricted spatial scope. One element of this co-ordination is the restricted spatial scope of application; this can also be described as the downside of the concept of sovereignty (see above). The Westphalian concept of sovereignty is based on the reciprocal acknowledgement of sovereignty over, but not more than over, a state's territory.

Consequently, EU data protection legislation is restricted in spatial scope: It only applies within the EU, if processing takes place within the EU (Article 3[1] GDPR), if a person in the EU is monitored (Article 3[2][a] GDPR), or if processing is related to the EU Common Market (Article 3[2][b] GDPR; marketplace principle).

[21] Although framed here as sovereignty in a general sense, the EU is of course not sovereign in a strictly legal sense. [...]

[22] Friedmann, op cit, 60.

'Adequate level of protection' concept of the EU data protection legislation. A second element of co-ordination is the concept of the adequate level of protection in third countries (Arts. 44–49 GDPR).[23] If such a level of data protection is identified, the barrier which maintains the territorial legal grasp of EU legislation on personal data is lifted and lets data flow into the realm of another legislation.

The EU data protection legislation does not require an 'identical regime' but only an 'adequate level' which leaves room for other cultural backgrounds and other approaches to data protection and privacy.

Although the concept of adequate level of data protection dates back to the Data Protection Directive of 1995, no common criteria have emerged yet, nor has significant cross-cultural research been carried out.[24]

HARMONISATION

Thus, the EU data protection regime is a combination of the maintenance of its own standards in its own territory (sovereignty) and co-ordination with other legal systems —in this context especially with U.S. legislation— if they provide for an adequate level of data protection via the Privacy Shield. But there is a third dimension of solving information law regime conflicts: harmonisation.[25] As long as legal systems around the world give the same answers to the same questions, they do not conflict.

Except for a very small number of universal standards (human rights, war crimes, etc.), law is a matter for nation states. This is especially true for areas of law that relate to the technological level of a society and the cultural balance between the individual and society. Whilst heavily promoted in the few wild years of the Internet, it is now accepted that there is no such thing as universal cyber law.[26] However, what does exist is widely harmonised law in the IP sector (Berne Convention; Universal Copyright Convention) and common technical standards set by the International Telecommunications Union (ITU) and by the bodies governing the Internet (ICANN, IETF, etc.).

There are several ways to harmonise different legal systems with one another: either in a top-down approach, a bottom-up approach, a horizontal approach, or an imperial approach. Or one may combine all these approaches in a transnational multi-level and multi-stakeholder solution.[27]

[23] For differing aspects of the adequacy concept according to the language (English or French) see A-L Philouze, 'The EU-US Privacy Shield: Has Trust Been Restored?' (2017) 4 EDPL, 463, 471–472.

[24] L Determann, 'Datenschutz in den USA – Dichtung und Wahrheit' (2016) 9 Neue Zeitschrift für Verwaltungsrecht, 561, 562 et pass.

[25] With sympathy for the transatlantic harmonisation of various aspects, see D C Nunziato, 'Forget About It? Harmonizing European and American Protections for Privacy, Free Speech, and Due Process' in: R A Miller (ed), Privacy and Power, Cambridge, Cambridge University Press, 2017, 304–327.

[26] Cf. L Lessig, 'The Law of the Horse: What Cyberlaw Might Teach' (1999) 113 Harvard Law Review 501.

[27] See C Djeffal's presentation in this volume.

Top-down approach. The top-down approach to harmonising legal systems is characterised by government meetings and international conferencing which might eventually result in a convention or something similar. The findings and regulations from a convention then trickle down into the legal systems of the states. The same top-down mechanism forms the core of (regional) international or supranational organisations when they establish legal standards which apply to their member states and which have to be applied by them. Actually, the European Union in relation to its Member States is an example of such supranational rulemaking. This approach has not been very successful outside Europe so far because it depends on the willingness and readiness of the states involved. And most nations outside the EU have not been willing to adopt the idea and concept of data protection.

Bottom-up approach. The opposing approach to harmonise legal systems is from the bottom upwards. In this approach, it would be the task of the data subjects and the data controllers, the consumers, civil society and the Internet industries to establish common standards of data processing and data protection. Business practices and consumers' preferred data protection options as the result of market competition —the interaction of stakeholders— can harmonise standards in internationalised markets. However, so far we have not yet seen any competition for (high) data protection standards. The consumers' demand is obviously low, and the supply and offers of data protection-friendly solutions corresponds with this low level.

Horizontal approach. A third approach —somehow in the middle between the two already mentioned— can be described as a 'horizontal approach'. Relevant experts meet, talk, write, read and discuss. This takes place mainly in the scientific community, for example with the methods of comparative law. But in the business sector as well, communication between peers can produce uniform standards (e.g. best practices).

Imperial approach. A fourth approach is the imperial approach. Obviously, it is an aggravating circumstance, that both the EU and the U.S. show an 'imperial attitude' towards the question of privacy and data protection. The United States do not want to obstruct its flourishing Silicon Valley data industry, and the European Union does not need to show consideration for its non-existing data industry, but rather for European consumers.

The EU concept of allowing data transfer (only) if an adequate level of protection exists in the country of destination has an indirect effect of harmonisation, at least towards economically weaker countries and regions of the world.

We have now a comprehensive study of the way countries in Africa 'comply' with these EU standards.[28] They only adhere to these standards on the level of the books or, rather, of the official journals —and not on the ground. And it is a fact worth noticing that the handful of countries which are subject to a positive adequacy decision of the European Commission are either Western countries (Switzerland, Israel, New Zealand etc.) or countries without any data industry (e.g. Uruguay).

If you look at the list of countries that have an adequate level of data protection, you don't find major economies, you only find countries like Uruguay and New Zealand but you won't find South Korea, Japan, Russia or China; obviously, the imperial approach does not work with the U.S. because it only works if the other side is prepared to accept to give in and to surrender, which is not a typical American virtue.

CONCLUSION

The differences between the data privacy cultures on both sides of the Atlantic are obvious, although they become smaller in comparison to other cultures (Africa, Asia). These differences can be observed on the books and on the ground.

These differences have a huge practical impact because they affect the fuel of the Internet industry, or at least its consumer products. This has resulted in a cold economic war. The means of war is to establish one's own data standards within the realm of the other economic bloc —the U.S. by offering internet services designed to adhere to their standards, the EU by pressing for adequate standards in other countries. When analysing our subject, we first have to identify this layer of economic war rationale and logic.

If this primary layer of conflict is removed, we will see the three elements of a collision of laws problem: maintaining sovereignty, co-ordination of legal systems, and harmonisation of legal systems. Sorting the elements of Safe Harbour and Privacy Shield into these three categories helps to structure and analyse the problem. Working with, playing with and re-combining the elements from the three boxes might help to find a better scheme for the future.

[28] P Boshe, Data Protection Legal Reforms in Africa (University of Passau dissertation 2017, to be published in 2018); cf. A B Makulilo, 'African Accession to Council of Europe Privacy Convention 108' (2017) 6 Datenschutz und Datensicherheit, 364–367.

An Essay on the Future of Data Governance: Data Protection in the Face of Internet Fragmentation

CHRISTIAN DJEFFAL[1]

INTRODUCTION

Is data governance at the crossroads? The main argument of this essay is that data governance needs to go many places at the same time.[2] This argument will be made by looking at current developments in domestic and international data protection regulation.

One of the many challenges facing data governance is the future of data protection regulation. The central claim of this essay is that the current discourse needs to pay more attention to the fundamentals of the debate. A future model of data governance needs more dimensions to it. This increased complexity is necessary for multifaceted normative reasons. Data governance ought to mirror legitimacy. Without governance innovation, the internet as we know it will fragment. It will be like looking into a broken mirror.

THE INTERNET LOOKING INTO A BROKEN MIRROR

If the internet looked at itself in a mirror today, that mirror would be broken and breaking, mirroring one face in many different ways and revealing its many facets. What used to be a network of networks, a uniting and global infrastructure, is changing. What is left of the decentralised architecture of data flowing free across borders? In answering this question, millenials might not even consider the declaration of the independence of cyberspace.[3] This text might strike them as coming from another century, which technically it does. This picture is broken in many ways:

There is an increased fragmentation of the internet; measures are now being taken that seemed unthinkable before; countries and regions are choosing isolation. This can be seen in developments around the world, and particularly in China, Russia and in the rift between the US and Europe.

Russia has always had a very special internet landscape including its own search

[1] Dr. Christian Djeffal is postdoc and Project Manager at the Humboldt Institute of Internet and Society and coordinates the research area Global Constitutionalism of with Professor Dr. Dr. hc Ingolf Pernice. He focusses on issues of artificial intelligence and digital public administration.

[2] As will become clear, the term governance is used here broadly, encompassing different ideas without excluding any behaviour involving governing effects.

[3] J P Barlow, 'A Declaration of the Independence of Cyberspace', https://www.eff.org/de/cyberspace-independence, accessed 13 February 2018.

engine Yandex and its own social network VKontakte.[4] After having had distinct internet censorship policies, Russia went on to implement specific measures that call the idea of a global internet into question. International newspapers paid some attention to a Russian Act of Parliament frequently called the 'Data Localisation Act'.[5] This act requires certain service providers to store data exclusively on Russian territory. It has been famously enforced once against LinkedIn, which had to shut down its services in Russia.[6] What has attracted even more attention is the alleged plan of the Russian authorities to negotiate independent root name servers with other countries. Such a change in the Domain Name System could be used to set up an independent network.[7] A similar story could be told about China, where authorities are working towards the establishment of a separate network.

It could well be argued that a crack in the mirror is also developing along transatlantic lines. In the famous Schrems case, the ECJ invalidated the Safe Harbour Agreement that was the basis for the decision of the European Commission that there was an adequate protection of data in the United States.[8] Consequently, there was a need to negotiate a new arrangement.[9] Many times, it has looked like this important possibility to allow transatlantic data flows would be invalidated. The decision of the Court was said to have been prompted by the Snowden revelations. Looking at the transatlantic rifts, it is striking that the U.S. intelligence oversight law distinguishes between nationals and non-nationals.[10] This could also be seen as another rift in transatlantic relations. The Court decided that an agreement between the EU and Canada on the transfer of passenger name record data might not be concluded because several provisions were incompatible with fundamental rights in the European Union, in particular the fundamental right to respect for private life and the fundamental right to the protection of personal data.[11] Furthermore, the General Data Protection Regulation (GDPR)[12] extended the scope of application of European data protection law even for controllers or processors outside the

[4] This is explained in an essay by Kevin Limonier with a title that fits very well into the present narrative: 'Russia's homegrown Web: From Free Info Exchange to Kremlin Tool' Le Monde diplomatique (10. 2017), https://mondediplo.com/2017/10/07russian-internet, accessed 16 March 2018.

[5] A translation can be found here: https://pd.rkn.gov.ru/authority/p146/p191/.

[6] Adam Taylor, 'Russia moves to block professional networking site LinkedIn' Washington Post (17 November 2016), https://www.washingtonpost.com/news/worldviews/wp/2016/11/17/russia-moves-to-block-professional-networking-site-linkedin/, accessed 16 March 2018.

[7] Deutsche Welle, 'Russia moves toward creation of an independent internet', http://www.dw.com/en/russia-moves-toward-creation-of-an-independent-internet/a-42172902, accessed 16 March 2018.

[8] ECJ Judgment of the Court (Grand Chamber) of 6 October 2015 ECLI:EU:C:2015:650.

[9] Many details concerning the background can be found in Kai v Lewinski, 'Privacy Shield: Notdeich nach dem Pearl Harbor für die transatlantischen Datentransfers' (2016) 4 Europarecht 406.

[10] For further information see the contribution by Thorsten Wetzling in this volume.

[11] ECJ Opinion of the Court (Grand Chamber) of 26 July 2017 ECLI:EU:C:2017:592.

[12] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance).

European Union, if they provide goods or services or monitor the behaviour of subjects in the EU.[13] This provision, which became applicable on 25 May 2018, is another step towards states increasing their control over internet jurisdiction.

JURISDICTION AND THE INTERNET

Internet jurisdiction is a topic that has been very actively debated in recent years.[14] Therefore, we ought not to focus on the newness of the topic and the differences the internet is creating in that regard, but rather on the continuities of the law on jurisdiction. This is indeed a very traditional area of public international law dating back to classic authors like Hugo Grotius. Jurisdiction is a mirror of what power and accountability mean in international law. Where there is no jurisdiction, there can by definition be no responsibility, which might translate to legal accountability. The concept of jurisdiction mirrors power in that it describes the legal limits of the sphere in which certain actors are allowed to act. In some areas like the international law of the sea, the extent to which states can exercise power is indeed a contentious issue. This led to the development of customary international law. Building upon that, many states concluded the United Nations Convention on the Law of the Sea.[15] But it is also possible to view jurisdiction from the domestic perspective. From a national viewpoint, legal jurisdiction relates to questions of how far a state can extend its competences. Take questions of criminal jurisdiction: is it punishable by law if national X of state A is attacked abroad? Or if X attacks somebody abroad? If different countries assert jurisdiction, there can be competing claims. The task of international law is to regulate the competing claims and describe the circumstances in which a state or another actor can assert jurisdiction. The traditional doctrine of international law focused on the linking of jurisdiction to territory. Yet, there have always been disputes concerning jurisdiction. The Lotus case of the Permanent Court of International Arbitration dealt with a collision between two ships on the high seas.[16] As each ship was sailing under the flag of a different state, the Court had to determine whether one of the flag states had the right to assert jurisdiction over the captain of the ship of the other state. One metaphor that is frequently used to describe the thinking in the 19th century goes back to Max Huber, a Swiss international lawyer. He described states in their international relations as billiard balls. Even then, there were phenomena that could not easily be dealt with within one particular domestic jurisdiction. Transborder rivers gave rise to cooperation between

[13] Art. 3 Sec. 2 GDPR.

[14] For a general account see U Kohl, Jurisdiction and the Internet: Regulatory Competence over Online Activity (Cambridge, Cambridge University Press, 2007). Regarding data protection see C Kuner, 'Data protection law and international jurisdiction on the Internet (part 1)' (2010) 18(2) International Journal of Law and Information Technology, 176; id, 'Data protection law and international jurisdiction on the Internet (part 2)' (2010) 18(2) International Journal of Law and Information Technology, 227.

[15] United Nations Convention on the Law of the Sea of 10 December 1982, UNTS 1833 (p 3), 1834 (p 3), 1835 (p 3).

[16] S.S. Lotus (France v. Turkey), 1927 P.C.I.J. (ser. A) No. 10 (Sep. 7).

states. Countries figured that there had to be some form of cooperation. The International Telecommunications Union (ITU) and the International Postal Union (IPT) are among the oldest international organisations.[17] They also dealt with data flows, even though they were not digital. International organisations were places for constant cooperation between states. The states 'transferred' parts of their jurisdiction to those organisations. Yet, there are also other trends and discourses surrounding jurisdiction in international law. The doctrine of extraterritorial jurisdiction deals with the circumstances under which states can assert jurisdiction within another state. Universal jurisdiction addresses the question of whether there are legal norms that can or must be enforced by every state and the international community. One central concept challenging the territorial conception of jurisdiction is global commons. There has been a push, for example, to give universal protection to the Earth's atmosphere and to exclude it from the claims of any one particular actor.[18]

What is to be learned from these insights into international jurisdiction? Three major lessons can be summarised here. The first is that jurisdiction problems can spark governance innovation. The second is that jurisdiction is also connected with accountability. Thirdly, jurisdiction is the legal expression of power.

Jurisdictional problems sometimes require new solutions and fixes. As described above, technological developments prompted the rise of international organisations in international law. We see a striking parallel in the rise of multi-stakeholderism, which has become an important mode of internet governance.[19] The forum tackling the issue of jurisdiction is the Internet and Jurisdiction Policy Network and is coordinated by a Secretariat in Paris.[20] In the 19th century this would have been a congress with a permanent secretariat of state representatives. Today, it is a multi-stakeholder process uniting states, international organisations, civil society, academia, technical operators and internet platforms.

If this trend continues to spill over into other areas and organisations, it might ultimately turn out to be as big a development in global politics as international organisations were in the last century. Furthermore, it is important to keep in mind that jurisdiction is also a prerequisite for doing what is necessary. Generally speaking, an actor without jurisdiction cannot be held accountable from a legal perspective. Jurisdiction is also the permission to act. There have been discourses around an amendment of the Budapest Convention on Cyber Crime[21] to give states under certain circumstances the capacity

[17] M Vec, 'Kurze Geschichte des Technikrechts' in: R Schröder and M Schulte (eds), Handbuch des Technikrechts: Allgemeine Grundlagen Umweltrecht, Gentechnikrecht, Energierecht Telekommunikations- und Medienrecht Patentrecht, Computerrecht (Enzyklopädie der Rechts- und Staatswissenschaft, 2nd edn. Springer 2011) 44.

[18] First report on the protection of the atmosphere / prepared by Mr. Shinya Murase, Special Rapporteur, A/CN.4/667, International Law Commission, Sixty-sixth session, Geneva, 5 May-6 June and 7 July-8 August 2014.

[19] J Hofmann, 'Multi-stakeholderism in Internet governance: Putting a fiction into practice' (2016) 1(1) Journal of Cyber Policy, 29.

[20] https://www.internetjurisdiction.net/.

[21] Council of Europe Convention on Cybercrime concluded 23 November 2001, UNTS 2296 (p 167).

to act abroad in the context of prosecution. However, if states have no jurisdiction, they can do nothing. The third aspect that needs to be mentioned is that jurisdiction is a power play. Jurisdiction is the legal capacity to enforce domestic law. States sometimes have to compete for jurisdiction, which amounts to a legal power play. Jurisdiction also represents the ultimate capacity to prescribe norms and enforce them. There can be an active competition between different actors about who has the power to make and enforce rules.[22] Considering that we are dealing with jurisdiction over data flows, this suggests that we are also dealing with power over those data flows. Power, however, ought to be exercised only where it is legitimate.

LEGITIMACY

The developments described here call for a reconsideration of the current internet governance. The internet causes deep structural changes,[23] and is itself subject to deep structural modifications. These changes in turn influence society. Before determining the question of jurisdiction over data flows and therefore governance over the internet, it is important to gain an understanding of their legitimacy in order to identify what measures to take. 'Legitimacy deficits' can call for new measures.[24] In this endeavour, it is not possible to rely on a single source or concept of legitimacy. It is, rather, important to have mixed conceptions that take account of the different forms of legitimacy.[25] This mix has to be prevalent on different levels. There cannot be one single form of legitimacy. Input or consent is one important element. The persons to which the data relate have to be in the loop in one way or another. Furthermore, output and effects are also important. The best rules and rights on data protection have no value if they do not achieve their goals in the real world. The best human rights on privacy and data protection are worth nothing more than the paper they are written on if they are not part of a living constitution. The mix also has to be prevalent when it comes to legitimacy through process. There is not one single layer in the multi-layer governance structure at which all data protection questions can be solved.[26]

[22] The accountability problem is actually the flipside of this: in cases where there are competing claims, often no actor wants to assert or exercise jurisdictions. Consequently, the problem remains unsolved.

[23] I Pernice, 'Informationsgesellschaft und Politik: Vom Neuen Strukturwandel der Öffentlichkeit zur Global Privacy Governance' (2013) HIIG Discussion Paper Series; id, 'Global Constitutionalism and the Internet: Taking People Seriously' in R Hofmann and S Kadelbach (eds), Law beyond the state: Pasts and futures (Normative Orders, Vol 18. Campus Verlag, 2016).

[24] See, for example, I Pernice, 'E-Government and E-Democracy: Overcoming Legitimacy Deficits in a Digital Europe' (2016) HIIG Discussion Paper Series.

[25] Those forms are frequently referred to as input, output and procedure: see F Peter, 'Political Legitimacy' in E N Zalta (ed), The Stanford Encyclopedia of Philosophy.

[26] For an application of the multi-layer approach to internet governance see I Pernice, 'Multilevel constitutionalism and the crisis of democracy in Europe' (2015) 11(3) EuConst 541.

GOVERNANCE

International data governance ought to be modelled after the accepted standards of legitimacy. This essay argues that there ought to be a mix of different conceptions of legitimacy. In consequence, data governance has to be multifaceted and multi-dimensional in order to account for different strands of legitimacy in specific situations. It could well be argued that there is already a very diverse system. Looking at the way in which the GDPR deals with transfer of data beyond the borders of the European Union, there is already an interesting mix of measures making transborder data exchanges legal.[27] These transfers are legal if there is a decision stating that the other jurisdiction has adequate privacy protections. Furthermore, data processors can also obtain personal data when they give sufficient guarantees. This allows the transfer of data to one single processor. Another way is to set up recognised binding corporate rules within one entity. These rules allow the transfer of data throughout the whole organisation. In this spirit of adding multiple possibilities and dimensions to the governance of transborder data flows, there will be some suggestions and distinctions that could further the design of transnational data governance.

STRENGTHENING INDIVIDUAL DATA GOVERNANCE

The proposition that the individual is crucial in future data governance can have different meanings. Subjective rights to privacy and data protection are enshrined as fundamental and human rights on the domestic, regional and international levels. Privacy and data protection are acknowledged as basic and fundamental considerations applicable everywhere and for everyone. As is well known, the function of human rights is not just to prohibit violations by public entities. They also require active protection by states to shield against violations of third parties. These individual rights must be a cornerstone of international privacy governance. Yet we often forget that the individual is also the central actor in the sense that each individual has a potential power to govern her/his data that often seems not to be appreciated enough. The most important actor in data governance is the individual. There is a huge variety of choice between products and services, and between different settings regarding data governance.

This empowerment can be achieved through education, regulation and technology. Education plays an important role in allowing individuals to make informed choices concerning the use of their data. It has been frequently stressed that the means of education should go far beyond teaching data protection and cybersecurity in schools. One approach gaining more and more attention is the gamification of education.[28] The game 'Orwell' follows such an approach by putting the player in the shoes of an intelligence officer.[29] In this function, the player is supposed to do the following:

[27] See Arts. 44ff.

[28] A Hansch, C Newman and T Schildhauer, 'Fostering Engagement with Gamification: Review of Current Practices on Online Learning Platforms' (2015) HIIG Discussion Paper Series.

[29] For further information about the first episode see http://fellowtraveller.games/games/orwell-kaeoy/. The game has been awarded several prizes.

Investigate the digital lives of citizens: Search web pages, scour through social media posts, dating site profiles, news articles and blogs to find those responsible for a series of terror attacks.

Determine the relevance of the information: Only the information you provide will be seen by the security forces and acted upon. You decide what gets seen and what does not, influencing how the suspects will be perceived.

Invade the private lives of suspects: Listen in on chat communications, read personal emails, hack PCs, pull medical files, make connections. Find the information you need to know.

Secure the freedom of The Nation: Find the terrorists so the citizens of The Nation can sleep safe, knowing Orwell is watching over them.[30]

The striking feature about Orwell is the change of perspective. The player is now in a position to access data, and s/he can see what can be learned from data on ordinary social networks. While investigating and learning about several individuals on the net, the player forms an understanding of what those data can mean when analysed.

Technology can empower human beings to exercise their human rights. The rise of artificial intelligence (AI), in particular, might play an important role in empowering individuals to exercise their rights. The chatbot 'Chommy', for example, allows individuals to obtain information about a data subject's personal data on the internet and in the future might also make it possible to organise the data according to the wishes of the data subject. There are many creative ways to develop these ideas in the future. Suppose that an artificial agent has a regular 5-minute real world conversation and identifies your perspective on data protection from it in order to change the settings of all the services you use accordingly.

[30] See the feature description of the game at http://fellowtraveller.games/games/orwell-kaeoy/.

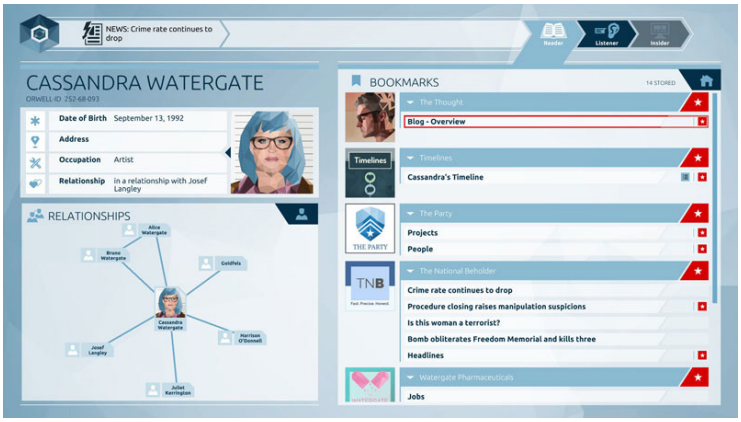


Figure 1: Screenshot from Orwell[31]

The particular design of services can also have aspects that empower individuals. One approach would be, for example, to have the possibility of paying for privacy (PPP). This would apply to services that use customer data to create value. They would be required to offer the opportunity for users to pay for the service instead of paying with their data. Golem.de, one of the leading German news sites on IT issues, allows for such a model. It is possible to use the site without advertisements, tracking and profiling for a monthly payment of €2.50.[32] The same is done by the leading Austrian newspaper 'der Standard'. For €1 per month, the site can be accessed without advertising and tracking. This could prove beneficial for businesses, too. They could attract more sceptical customers with different business models. There are currently many projects that are planning to build a micropayment ecosystem making it possible to finance online services. The browser project Brave[33] is trying to establish a specific crypto-payment system to do this.[34] More initiatives heading in the same direction are on the way.[35]

[31] http://fellowtraveller.games/games/orwell-kaeoy/.

[32] Golem.de, 'Golem.de startet werbefreies Abomodell', https://www.golem.de/news/golem-pur-golem-de-startet-werbefreies-abomodell-1408-107827.html, accessed 19 March 2018.

[33] https://www.brave.com/index.

[34] S Shankland, 'Brave browser begins million-dollar token giveaway: You won't get more than about $5 worth of tokens, but the browser maker hopes you'll help improve online advertising privacy.' (17 January 2018) https://www.cnet.com/news/brave-browser-begins-million-dollar-token-giveaway/, accessed 19 March 2018.

[35] The company Eyeo is trying to do the same with an adblocker and a specific paying service. The Berlin start-up Satoshipay is also making an attempt to establish a micro-payment model. For a summary see T Kleinz, 'Brave-Browser: Adblocker mit Bezahlfunktion per Bitcoin' (2 September 2016), https://www.heise.de/newsticker/meldung/Brave-Browser-Adblocker-mit-Bezahlfunktion-per-Bitcoin-3312905.html, accessed 19 March 2018.

Regulation can have many impacts on individuals. It can allow individuals to claim damages and enforce rights before courts. Regulation can, however, also change the game through other ideas.

MULTIPLE LAYERS AND ACTORS

As with other globally relevant topics, data protection can be dealt with on different levels: the domestic, the regional and the international. On each level, there can be multi-stakeholder participation. Take, for example, the United Nations. The General Assembly of the United Nations has taken up the issue of data protection for the organisation of the United Nations,[36] but has also reacted to the problem of surveillance by states. The process started with Resolution 68/167,[37] which instituted a Special Rapporteur on the right to privacy. This rapporteur has recently published a draft Legal Instrument on Government-led Surveillance and Privacy.[38] This is striking since he wants to account for the surveillance not only of intelligence agencies but also law-enforcement agencies. It is also a striking attempt to formulate rules and principles for very different settings. The provision also lays great emphasis on privacy-enhancing technologies in the surveillance context.

Questions of data protection play a big role in several fora like the Internet Governance Forum (IGF) and the related regional fora. The IGF is a discussion platform organised by the United Nations. At the 2017 IGF in Geneva, there were several sessions focusing on data protection.[39] By nature, discussion platforms do not take individual decisions.

One regional initiative is the Asia Pacific Privacy Authorities.[40] Since 1992, they have combined the data protection authorities of Asia-Pacific countries as well as the US, Colombia and Canada. This initiative has the aim of furthering privacy in all countries and establishing cooperative arrangements between the authorities and the countries. The Council of Europe is another interesting forum in that its Convention on Data Protection[41] has gained general acceptance in Europe. More interestingly, four states which are not members of the Council of Europe —Mauritius, Senegal, Tunisia and Uruguay— have recently acceded to the treaty and accepted the standards. More Latin American and Af-

[36] See General Assembly resolution 'Guidelines for the regulation of computerized personal data files' 45/95 of 15 December 1989.

[37] Resolution A/RES/68/167 'The right to privacy in the digital age'.

[38] Ver. 0.7 of 28 February 2018, available at http://www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/2018AnnualReportAppendix7.pdf.

[39] See the programme at Internet Governance Forum https://www.intgovforum.org/multilingual/content/igf-2017-geneva-switzerland-18-21-december, accessed 13 February 2018 (n 22).

[40] Asia Pacific Privacy Authorities: for more information see http://www.appaforum.org/, accessed 13 February 2018 (n 23).

[41] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, concluded 28.01.1981, entered into force 01.10.1985, ETS No.108.

rican states are currently considering joining. This might be an interesting development in common privacy standards between states. However, there are also bilateral developments like the Privacy Shield agreement or the European Canadian Treaty on Passenger Data. Questions of data protection are neither determined by one class of actors nor on one particular level of governance. With this in mind, it is always important to look at what level of governance is best suited to deal with certain challenges of data governance. In the end, the ultimate standard of data governance is the empowerment of the individual to effectively exercise his/her rights. All rights and protections on all layers are worth nothing when individuals do not know what is at stake. Informed choices by individuals are the basis for a good and sustainable data governance, which is beneficial to all actors and stakeholders in society.

GDPR, Privacy Shield and the Framework Agreement: A US Perspective

ZACHARY K. GOLDMAN

Thank you everyone for coming, and yesterday's conversation was so rich it caused me to throw out everything I was going to say and work on something new to contribute to the discussion. So, what I have is perhaps a bit provocative, and I hope you will either agree with me or disagree with me —preferably disagree with me, and tell me why I am wrong— and I hope we can find a solution. But what I was thinking about a lot is the source of continuing tension about privacy, given the obviously very close economic, political and socio-historical ties between the US and the EU, and what I actually believe in practice to be rather similar privacy regimes.

A foundational concept is that there is a particular set of institutions in the EU that by constitutional design divorce consideration of commercial data privacy from national security issues at two levels: the first, and most obvious, is within the EU itself, which has no competence over national security issues —that is, a competence that has been left with the Member States, and that means that the ECJ has no competence over national security. When you contrast this with US courts, the differences can be quite stark. In their fourth amendment analysis and other contexts, US courts regularly engage in a kind of balancing test, where they weight privacy interests of individuals against national security interests of the state, and they are able to make these kinds of calculations because the courts in the US have jurisdiction over both sets of issues. And second, both at the EU level and at the national level with the DPAs, that kind of weighing and balancing does not take place because the national-level DPAs have no jurisdiction over anything other than data privacy. I think that is a product of the fact that data privacy and data protection are understood as a fundamental right, and so, if it is a fundamental right, then no weighing and balancing can take place —fundamental rights must be protected to the maximum level. So, I suppose when I think about it, the concept of the fundamental right is one aspect, but then really the translation of that fundamental right concept into a set of institutional arrangements that separate, as a matter of constitutional law, national security from commercial issues relating to data privacy seems to be doing a lot of work.

With these as my foundational precepts, I kind of have three assumptions and then four provocations that I wanted to offer about how to think about this problem moving forward.

So, the three assumptions: first, what the ECJ really does not like is the idea that Europeans can be treated like residents of a hostile regime (e.g. Iran or North Korea) for surveillance purposes, which is to say that as non-US persons outside the United States Europeans have few legal protections in US courts with respect to foreign intelligence surveillance (and certainly far fewer protections than those available to US persons or persons inside the US). And the ECJ at some level, as a supranational body, has a hard time accepting the legitimacy of distinctions drawn in this way, particularly as they affect people whose rights the ECJ is supposed to protect. Thus, one assumption is that what the ECJ does not like in the Schrems case —and in the Schrems case that is about to come— is the core of the legal architecture of US surveillance. The second assumption is that the foreign intelligence surveillance regime of basically every other European country looks exactly like that of the United States, which is to say, people inside the country and nationals anywhere in the world have rights, but foreigners outside the country have no rights (or dramatically reduced rights). So, for example, Germans inside Germany have no rights vis-à-vis the French or the Italian intelligence services, and the French and the Italians inside France and Italy have no rights vis-a-vis the UK intelligence services. Germany is the one exception to this rule, as Thorsten Wetzling told us yesterday, in the new surveillance law that Germany just adopted. And the third assumption is that the commercial data privacy regimes in the US and in the EU, notwithstanding the substantial institutional differences, are in fact essentially equivalent. Therefore, setting aside the national security issues for a moment, if you look at the developing jurisprudence of the FTC, and the Department of Health and Human Services, and the Food and Drug Administration, and the other US agencies that are charged with what would be called data protection here, what is in the US privacy law, it can be seen that the fundamentals of the legal regime are more or less the same, similar, certainly essentially equivalent. I would argue that the US is developing a richer and more robust privacy regime that looks an awful lot like Europe's.

So, those are my three assumptions. Consequently, if that is all right, or even reasonably close to right, then I have four provocations about where we go from here. The first is that the ECJ simply carves national security considerations with respect to the US out of its thinking about data privacy cases, just like it cannot consider national security issues that have bubbled up from the European courts because, again, it is not a matter of EU competence and therefore not a matter of ECJ competence.

Second, and this is perhaps a kind of research agenda for this group moving forward, is to add substantially more detail to this concept of essential equivalence, and to figure out exactly what we mean when we say, a data privacy regime must be essentially equivalent. If the second Schrems case is going to come out like the first Schrems case, and if the SWIFT agreement and the PNR agreement are about to fall because of data privacy concerns, then what that means is that the EU and the US cannot sustain a data

transfer agreement of any kind. If it is true that the EU and the US cannot sustain a data transfer agreement of any kind, then I do not know with whom the EU could sustain a data transfer agreement —certainly not Russia, certainly not China, certainly not most countries in Africa, certainly not in the Middle East, and certainly not in much of Asia. Accordingly, if that is true, then Europe becomes kind of a data island, but I am not really sure what that means for the economic and commercial future of the continent. So, that, in my mind, cannot be the case, it cannot be the case that no EU-US agreement on data transfers is possible, because of what that implies for the ability of Europe to reach data transfer agreements frankly with anybody. So the second provocation is let us figure out what essentially equivalent means to facilitate a sustainable data transfer regime between the US and Europe.

The third provocation is: let us come to a common understanding of what we mean by harm in the data privacy as well as data protection space, and maybe this is part of the second of what it means to be essentially equivalent. But I assume that we are operating under potentially quite different understandings of the concept of harm in the data privacy space, and I think that at least making explicit these different visions of harm certainly would assist in understanding. And I say this fully cognisant of the fact that within the US, there is not necessarily a real common vision of what we understand to be harms in the privacy space. Therefore, if you look at the case law in the data breach context surrounding who gets to get into court, the idea of standing, who has been harmed sufficiently to bring a suit in the event of a data privacy incident —there is no harmonisation among different legal regimes. So, the FTC has answered that question differently than the Article III Courts have answered it, and among Article III Courts, they have answered that question differently. But I think, a better understanding of what we mean when we talk about what we are trying to protect against would really be beneficial.

And the fourth provocation is if the ECJ does seek to somehow evaluate the national security practices of the United States, I would hope that they can take at least a holistic view of the intelligence regime in the US. This would include not only the legal authorities under which it operates, but also the oversight regime to which it is subject. So when the ECJ reviewed Section 702 of the FAA, they looked at this law but did not take a holistic view of the institutions and mechanisms of oversight that accompany the law. And I think that any informed discussion of intelligence practices has to take into account both the scope of the authority and the oversight mechanisms that are in place to police compliance with the authority, because I think if you look at the documents that have been made public in the last couple of years from the foreign intelligence surveillance court, you see a remarkable level of engagement by the courts in establishing sets of rules by which the intelligence agencies have to operate, and then policing compliance with those rules on an ongoing basis. And this dialogue between the surveillance agencies and the courts over the last decade —most of which was taking place in total secrecy until two or three years ago, which is actually quite remarkable— I would posit exists nowhere else in the world.

Discussion: GDPR, Privacy Shield and the Framework Agreement

MARIE-CHRISTINE DÄHN

The conference's second session focused on possible approaches for establishing a common ground in the transatlantic legal framework as well as data protection and privacy practices. In its first block, the participants reflected upon Europe's upcoming General Data Protection Regulation (GDPR), the EU–U.S. Privacy Shield and the 2015 Framework Agreement mainly from the European and US perspectives. Following the inputs by Kai von Lewinski, Zachary K. Goldman, and Christian Djeffal, a lively debate ensued.

Perhaps one of the most significant observations to be made in the debate was that, from a practical perspective, it would be most counterproductive if regulations —not only in the European Union or the United States but also globally— fragment the internet (in the debates labelled as 'balkanisation of the internet') so that a patchwork of isolated single rights, access rules, and laws creates national borders virtually. In this regard, China has been mentioned as a telling example since it has its own data infrastructure and internet in the national realm, which proves to be not very cost-effective. It is, moreover, imperative that mutual new restrictions and frameworks for problems in new contexts, like massive data collection in big data settings, are found to address emerging issues jointly on both sides of the Atlantic because the problems arising affect not only single states. In addition, fragmenting the internet would not work out over the long term because it would be avoided: individuals and companies would establish what they do elsewhere where a free (global) flow of data would be possible and entrenched. This could lead to a kind of forum shopping for different privacy protection rules so that companies would establish subsidiaries in other jurisdictions where the legal system reflects their interests. To counter this, it has been suspected that privacy and data protection might serve as a cue for industrial aims. Nevertheless, a consensus was reached in the discussion that a merely polarised debate would be pointless.

In defining the rules and norms in place, courts play a substantial role. They address the most pressing issues as they are confronted with the cases put forward to them. In this regard, the participants elaborated, courts in the U.S. and the EU primarily protect privacy and security, whereby the European Court of Human Rights (ECtHR) is especially clear in its rulings on national security since it puts emphasis on the protection of fundamental rights. But generally, in the EU and the U.S. alike, cyber security is not excluded from legal considerations. For Europe in particular, the participants pointed out, data processing by intelligence agencies is not covered by the GDPR, for national

security issues falling exclusively under Member States' legislation (TEU Art 4, 2.), and so far, no case on intelligence services' activities has been brought before the European Court of Justice (ECJ). Most importantly for the ECJ, national security issues are beyond its jurisdiction, therefore, it cannot address them properly. So that narrows the focus in Europe. Nevertheless, the ECJ plays an important part in these discussions on security, privacy, and data protection, as can be seen from the modes of harmonisation and balancing approaches in the Court's cases. Over the years, the ECJ's cases used the Data Protection Directive 95/46/EC as a primary basis, and apart from this there have not been many changes. Yet its importance is underlined as the ECJ has the ability to challenge surveillance practices in a direct way by its rulings and the attendees remarked that pressure could be created in courts, such as the ECtHR.

It is crucial, as became clear in the comparison of European and U.S. practices and frameworks, that if one wants to understand the transatlantic relations with respect to privacy, data protection, and security, one has to understand the actor's intentions. What has to be kept in mind in this regard, however, is the different understandings of privacy and data protection, as well as the different approaches underlying the respective legal frameworks. These differences are not only grounded in the respective legal histories. One participant pointed out that at some point, the legal debate on the one hand and the philosophical, sociological and political debate on the other seem to have been moving apart for many years, with the legal discourse oftentimes being very self-referential. In addition, cultural ideas and developments have to be taken into account to further the understanding. The perception that the U.S. is controlling the direction in which the EU is heading has been emphasised as being particularly problematic. The overarching culture of secrecy is one of the core characteristics of services and their functioning. This heavily influences the debate, too. It was claimed by some participants that this has to be overcome and be replaced, instead, by a culture of trust, building on enhanced knowledge and mutual confidence.

To enforce a coherent framework, the competences of oversights need to be clear. The GDPR in Europe enhances the supervisory powers of Data Protection Authorities (DPAs) in its sixth chapter (Arts. 55, 58). In the case of the U.S., on the other hand, the participants did not reach an agreement on how to strengthen oversight competences best. One idea, which was already raised by the European Article 29 Working Party, is to create or strengthen an oversight board, like the Privacy and Civil Liberties Oversight Board established by the U.S. Congress in 2004, and to appoint an ombudsperson responsible for issues in this realm. Such an ombudsperson to be appointed under the Privacy Shield deals with data protection complaints by EU citizens. The Under Secretary of State for Economic Growth, Energy, and the Environment actually holds this office in the U.S.. However, the discussants remarked that an extension or generalisation of such an institution would be an improvement. This could be a step forward towards a joint approach.

A major difference between the U.S. and the EU approaches to regulating privacy and cyber security —one that has been pointed out repeatedly in the debate— concerns the foundation upon which the law rests. While a European understanding and interpretation is based on a comprehensive constitutional framework on which proponents base their arguments, the U.S. focuses on the ethical considerations and debates as an orientation for legal reasoning. For instance, in the EU, privacy and data protection are enshrined as two different fundamental constitutional rights of their own (Charter of Fundamental Rights of the European Union, Arts. 7, 8). In the Lisbon Treaty of 2009, i.e. the Treaty on the Functioning of the EU, as well as in the European Charter of Fundamental Rights, these rights are not only codified but also clarify the core legal instruments to achieve protection. This is further pursued by many legal frameworks of individual Member States which the GDPR is going to replace in order to achieve an equal level of protection throughout the Union. Although these foundations seem straightforward, the discussion unearthed a dispute regarding the constitutional derivation of privacy and data protection in European law. Some participants, following Whitman (2006), understood the European concept of privacy as deriving from human dignity, while others challenged this understanding by referring to the German Constitutional Court's census decision (1983), arguing that privacy and informational self-determination are a particular manifestation of individual freedom. In the U.S., individual freedom also plays a key role in privacy and data protection as they are based on conceptions of autonomy and liberty, which are codified in the Bill of Rights and the U.S. Constitution. The First and Fourth Amendment of the Constitution are essential pillars of these rights. Nevertheless, the U.S. legal framework is also significantly shaped by civil court decisions as privacy and data protection are not completely codified and elaborated in the Constitution. In Europe, in comparison, it is mainly the constitutional courts that advance the development of the legal framework in this regard. Various privacy statutes and acts, like the Privacy Act of 1974, further elaborate the U.S. privacy and data protection understanding. More generally, a dichotomous juxtaposition of the notion of freedom in the U.S. and fundamental rights in the EU as the legal frameworks' foundations was considered by some as problematic. Rather, taking these differences into account, there was a general agreement among participants that an approach of mutual learning between the EU and U.S. would be most fruitful.

One attempt to do this mentioned by a participant is the 'EU-US Privacy Bridges' project, which brings together EU and U.S. privacy experts in order to find practical solutions that may bring both approaches and practices closer together. It is aimed at advancing the development of global privacy rules on the one hand, and advancing relations between the U.S. and EU perspectives on the other, while also taking differences between the two jurisdictions as well as the shared goal of effective privacy protection seriously.

In practice, the discussants emphasised that legal and non-legal instruments need to be flexible enough to cope with the different (legal) transatlantic contexts. A necessary component of this would be the differentiation and assessment of possible distinct instruments, together with their regulatory impact and their side effects. Instruments that might seem appropriate in one context could in fact increase cyber risks or could grant unauthorised access to data in others. Participants stressed that further debate is also needed with regard to the risks and presumed dangers. The debate was divided on the question of whether, for example, government surveillance should be rated as one of the most pressing issues, or hackings by criminals. What became clear, however, is that none of the possible threats should be completely neglected.

Cyber Security Cooperation on the Ground

SVEN HERPIG

This abstract provides a brief overview about selected forms of formal and informal, technical and political cyber security cooperation, as well as an outline of the setup and work of the Transatlantic Cyber Forum (TCF) as a different model for cyber security cooperation.[1]

To start with, it is useful to point out what cyber security cooperation can mean, and on what levels we experience it, as well as what forms of cyber security cooperation currently exist. First of all, there is international cooperation. On the United Nations level, there is the governmental group of experts (UN GGE) on cyber norms.[2] Secondly, there is the transnational level, which includes more than one member state of the United Nations, but could also include non-state actors, such as international cyber security companies or non-government organisations. The currently most-debated transnational cyber security co-operations are Microsoft's Geneva Convention[3] and the approach of the Carnegie Endowment of International Peace (CEIP)[4] to stability of the international financial markets vis-à-vis cyber threats. Compared to the UN GGE process, CEIP focuses solely on the stability of the international finance sector and within that, it (first) targets the G20 circle of states. From there it might broaden out to create something like an international agreement to enhance international cyber security.

Then there is regional cooperation. On the NATO level, there is, for example, the so-called locked shields exercise,[5] which is a cyber security/ cyber defence exercise. Moreover, there is the Tallinn Manual[6] of the NATO Cooperative Cyber Defence Centre of Excellence (CCD COE) and there are the confidence-building measures[7] of the Organisation for Security and Co-operation in Europe (OSCE). All of this is regional cyber security cooperation.

[1] More information available at https://www.stiftung-nv.de/en/project/international-cyber-security-policy.

[2] https://ccdcoe.org/back-square-one-fifth-un-gge-fails-submit-conclusive-report-un-general- assembly.html.

[3] https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/.

[4] http://carnegieendowment.org/programs/cyber/.

[5] For more information see https://ccdcoe.org/event/cyber-defence-exercises.html.

[6] The manual is available at: https://ccdcoe.org/tallinn-manual.html.

[7] See http://www.osce.org/secretariat/cyber-ict-security.

On the European level, there are different frameworks that foster cyber security cooperation. The Directive on security of network and information systems (NIS Directive)[8] which led to the EU CSIRT network[9] comes to mind, as well as the EU cybersecurity strategy.[10]

Multilateral cyber security cooperation is less known to the policy circles. There are initiatives such as SOG-IS MRA[11] or the EGC group. SOG-IS MRA is the senior officials' group for information security mutual recognition agreement. This is a sub-group of European Union states which certify, for example, hardware; when that hardware is certified by one of the members of this group, other members can use that certified hardware without having to certify it again. So, each participating country recognises the certification of the other participating countries. The EGC group is basically a group of certain computer emergency response teams (CERTs), from countries such as Germany, France and the Netherlands, who share privileged information about, for example, cyber attacks.

Furthermore, there is bilateral cyber security cooperation. One form of this that has been discussed repeatedly in German, US and other international media was the German-French policy cooperation on crypto-regulation. In 2016, there were high-level talks between Germany and France about how to pursue crypto-regulation together on the European level.[12] Another example of bilateral cyber security cooperation would be the US-Chinese agreement on cyber crime.[13]

And then there is 'national cooperation': national good or best practices that can be adopted and adapted by other states. Germany created the so-called 'IT-Grundschutz', which in its first version was a catalogue of security mechanisms for certain types of software and hardware. Companies can obtain a certificate declaring that they comply with IT-Grundschutz's standards. The Estonians have adapted and adopted the IT-Grundschutz in order to foster their own national cyber security.[14] One state created something, made it a best practice and then other states that may have less resources in that area can adapt and adopt it.

How does the Transatlantic Cyber Forum fare in that list of cyber security cooperations? TCF brings together German, American and other EU cyber security practitioners and experts from the private sector, academia, and civil society. These experts are working in three working groups, or 'tracks', to solve policy changes that take place in the respective countries. The first working group focuses on government encryption policies

[8] https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive.

[9] https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services/cii/nis-directive.

[10] More information available at https://ec.europa.eu/digital-single-market/en/policies/cybersecurity.

[11] https://www.sogis.org/.

[12] For detailed information see https://regmedia.co.uk/2017/02/28/french_german_eu_letter.pdf.

[13] For a discussion of the agreement see https://fas.org/sgp/crs/row/IN10376.pdf.

[14] https://www.ria.ee/en/iske-en.html.

and government hacking; right now, together with the experts, it is focusing on creating a 'gold standard' for vulnerability management mechanisms[15], based on the lessons learned from the US vulnerability equities process (VEP). At the same time, the group is working towards creating minimum standards for government hacking, including authorisation, oversight, transparency, securing hacking tools and more. The second working group[16] discusses ideas for securing democracy in cyberspace by addressing challenges for data-driven elections in an adversarial geopolitical space. The group is analysing what kind of data will be used for campaigning and elections and how it has been targeted in the past for what purposes. All this permits the group to anticipate possible threats to those elections and ultimately leads to the design of appropriate safeguards and security mechanisms. The third track[17] deals with oversight innovation and intelligence governance, focusing on the topics of improved accountability of intelligence oversight, as well as technological improvements for better governance in that area.

TCF has a slightly transnational approach because the working groups include not only representatives from the private sector, academia and civil society but also former government employees. The drafts of the policy papers are also shared with current officials for comments. The TCF takes a comparative look at the respective countries and then brings the best parts together while adding some aspects that this group of practitioners would like to see. All this is then moulded into policy products. It is basically a best practice (trans-) national comparative approach. In other words, the experts work together and learn from each other, and create policy products that can be replicated. The Internet and the underlying technology is the same everywhere, therefore the respective policy discussions lead to similar challenges. Thus, it allows the group to create options that can potentially be adapted and adopted globally. Apart from the challenges currently being tackled by the TCF, there are many more in the realm of cyber security, such as hack backs, protection of critical infrastructures, responses to adversarial cyber operations, attribution, emerging technologies or human resources shortage in the IT security field. All of these challenges are in dire need of good models that will allow states to alleviate them.

A word of caution though: Creating national best practices to be replicated elsewhere can have unintended international consequences. The so-called normative spillover effects occur when a policy that is implemented in one country leads to a perversion of that policy in another country while that country will respond to all diplomatic inquiries by saying: 'But you are also doing it'.

[15] For more information see: https://www.stiftung-nv.de/en/project/international-cyber-security-policy#erstens.

[16] See https://www.stiftung-nv.de/en/project/international-cyber-security-policy#zweitens.

[17] See https://www.stiftung-nv.de/en/project/international-cyber-security-policy#drei.

Cyber Security and Privacy Protection as Global Challenges: What Role for the U.S./EU Partnership? – A German-American Perspective –

PHILIPP KRÜGER

I'm an advisor at Fraunhofer SIT and have been part of CRISP for some years, which is one of three national cyber security research clusters. I'm also an advisor at the German Ministry of Defence. But I think the reason why Ingolf Pernice invited me today is that I lived in the U.S. for 12 years, working in NYC and Cambridge and researching at Harvard and MIT, and my wife is American and my son has a German and U.S. passport. So I have a personal incentive to make that transatlantic relationship work.

Today I want to talk a little bit about what I perceive as a bias that we have towards potential collaboration and perhaps a realistic approach when it comes to what could be a couple of lighthouse projects where the U.S. and Germany could actually collaborate, and I am going to start with a quote from my dad. I spoke with him yesterday, before this, and he worked for Siemens all his life in med-tech and he told me: 'Philip, that is a tough world for you guys today in digital society, because back in my day in med-tech it was Phillips and Siemens and General Electric, and we would sit around the table and we would set the standards; but today, for you, it is pretty difficult, especially if you look at it from the German perspective towards the internet, but not so difficult for the Americans to set standards'.

Hence, I think, this has led to a bias in Germany towards more regulation, and on the other side, in the U.S., there is a bit of a bias towards market forces. And in reality, I fear it has led to a situation where we do not have rules for the road, we do not have global governance in the digital landscape, and we might have a couple of bilateral agreements but we have major disagreements, for example when it comes to something like the Wassenaar agreement, VEP, or also how to scale products and services globally.

So, there is a lot of disagreement, I think, under the surface. Thus, I want to talk a little bit more about other levers that we might use beyond regulation, while certainly I hope that in the long term we will get to global governance. So, call it a more realistic approach. I am going to talk about money and power. I want to talk first about economic collaboration and then about cyber deterrence collaboration and then at the end very shortly talk about three or four actual projects that we might be able to collaborate on.

First of all, I want to start with economic collaboration in the digital realm. I think all of us know that the U.S. controls the technology market's standards, mostly going deep into the OSI layer, backbone devices, operating systems, content platforms —we do not

have much of that in Germany, we have SAP but that is it. This then leads to a situation where Germany and also the EU, to a certain extent, is a second mover in cyberspace, in the global markets, and is extremely reliant on 'Fremdcode' or the so-called 'Fremdhardware', which has led to a situation where we do not really have what Klaus Homme —he is one of the leading investors here in Germany— called 'cross-platform competence'. Consequently, we do not have the Ubers, we do not have Google, autonomous driving stuff, because we already do not have the platforms to begin with that we could then combine to come up with a new business model or new technology.

So, there is a problem for Germany, and it is even more problematic because we have fantastic scientists and computer science. They just sometimes leave or come back, but if they want to scale something here it does not really work, and so that is a problem. Then we have security issues if the show is run by someone else in terms of how secure our data is, how secure the stuff is, and then we very much move towards discussions like those on encryption and regulation. That is what we have been doing for a long time.

What is ahead, I think, is that this might change because a couple of things are changing: one is that the U.S. is facing international competition; there has been a bit of a levelling of the cyber playing field, and we see what China is doing, especially in artificial intelligence, machine learning, deep learning, and neural networks. Fraunhofer SIT has just opened a partner office in Israel, and now in Singapore, so we have quite a few scientists from there, and they are doing fantastic work. The Russians have become pretty sophisticated in terms of what they can do, i.e. when they attack in an election. So, there is a bit of competition for the U.S., and we are also now seeing a trend within the U.S. towards more regulation. Therefore, that is kind of new, and on the other side, in Germany, and in the European Union they are actually considering spending some serious money on things like disruptive innovation or cyber commands, and things like consortiums of large companies, Siemens, Daimler, Intel, or HERE.

So, there is a little bit of action going on here, because I think a couple of players are also realising that if we miss the Big Data train and some other trains, then it is said that German manufacturers, even car manufacturers, will not be able to charge a premium for the label 'made in Germany' anymore in the future. If the digital component has become so important, and if the digital component is not in our hands but in others' hands, then why would anyone pay a premium for a German product anymore?

As can be seen, there is some awakening, and this might lead to actual collaboration in terms of projects, and I am going to talk about one of these that I find interesting which is collaboration when it comes to Big Data. There is a project here in Berlin called 'HERE', not far away from here; it is between Daimler and, for example, Intel and a couple of others, and it is addressing the issue of how you can build something like a Google Maps within the German innovation framework. This is an interesting project.

A second point is collaboration in regard to power or conflict —I call it cyber deterrence collaboration. I think here —that is quite interesting too— something has changed.

We have had some kind of Sputnik moments in the past, you could take Stuxnet, then perhaps Edward Snowden. So, the world has awakened to what some players can do in this space, and now we see an arms race, and other players that were second have moved up the value chain, and they can now compete in certain areas of operation with the U.S., and this leads to the question: how will Germany, as a mid-ranked power itself, behave in that scenario of escalation dynamics in cyberspace?

And there is quite something happening right now when it comes to the new German cyber command and when it comes to new clusters and new innovation mechanisms.

Let me add some final points about cyber deterrence: I think we have to be careful here again not to be biased when we talk about cyber deterrence. In the past, we talked about nuclear deterrence and we were trying not to apply some of these lessons learned to this new scheme. It took about 20 years until we had the non-proliferation treaty. Now, let us say, we are at least 20 years into the digital revolution, and we have nothing, we have a couple of bilateral agreements —China, the U.S., some talks between Germany and China, but basically, it is a Wild West out there when it comes to cyber deterrence. I think one of the reasons for this is that we have to be honest and admit that some of the stuff from the nuclear deterrence that we learned does not apply to cyber deterrence. So, I think one of the most interesting fields right now is what the escalation dynamics in cyberspace are and how you can build an effective system of cyber deterrence, and what role a country like Germany could play in this, and how it could collaborate with the U.S. on this.

Unfortunately, some brilliant people, like Joe Nye, who is at the forefront of this, have recently said that we do not see many rules emerging here on a global governance scheme, so we might have to try different ways, and one of the things I think that is worth looking at here is, for instance, how nations could collaborate when it comes to interoperability between their cyber commands. You see, for example, some of these efforts happening now between Germany and France.

We could also think about what cyber deterrence play books are used by the U.S. and whether this is something that Germany should use. So, there are a couple of areas where there could be collaboration but there should also be, I think, a little bit more research about the definition of cyber deterrence on both sides.

We also see that in Israel, for example, cyber deterrence means something like mowing the lawn, and that is something that probably does not work for Germany. In the U.S., in the very early days, we saw a bias towards defensive stands, then they got a little bit more offensive, now it is unclear where it stands, and in Germany it was the opposite. In Germany, traditionally our stand is more defensive, now it is becoming more offensive —at least, it is being discussed. So, where are areas where we could collaborate on this?

I think there are some good opportunities. One thing —because I come from a scientific background originally— in technology it is always easier to collaborate, and there are some projects on the way which have to do with creating, so to speak, a DARPA —an

agency for disruptive innovation in Germany or in the EU, and I think it is an interesting approach because technology is developing exponentially. Consequently, if you ever want to play a bigger role beyond regulation, perhaps you should come up with some products that are scalable, perhaps it should work on the market; and one asset that we have is good science. So why don't we focus a little bit more on disruptive innovation and reform a little bit or add a little bit to what is being done now, which is the classic process of incremental research, science, and Grundlagenforschung? So that is one area where there is stuff happening, Macron has just talked about it, and there might be something happening in Germany next year.

Another area I mentioned here is the company consortiums. HERE, I think, is a very good example, and another example of that is Siemens' Mindsphere, an interesting example of industrial IoT plus machine learning. Furthermore, there are a couple of U.S. firms involved, too. That is interesting, and another area is more collaboration between the two cyber commands; the U.S. cyber command used to be kind of a hybrid thing between Homeland Security, NSA and the Department of Defense, and only recently, a month or two ago, it was declared to be a single entity, we call it Teilstreitkraft, a single force within an operational space— land, air, now cyberspace. And the Americans, it took them ten years to figure this out, and make this and do that, while we created a cyber command per decree very recently and right away, and turned it into a Teilstreitkraft, without even knowing what that means and if we can do it.

As can be seen, there is a lot of work ahead of us, I think, whenever the U.S. and Germany collaborate in a meaningful way, that is a win-win situation. I am not so optimistic right now with regard to political framework and regulation attempts, but if we collaborate on the specific levels of science, research, innovation, market forces, cyber deterrence and startups, then I assume that it will be a win-win situation. I think there is reason for optimism.

Discussion: Cyber Security and Privacy Protection as Global Challenges: What Role for the U.S./EU Partnership?

MARIE-CHRISTINE DÄHN

In the second block of the conference's second session, the participants addressed cyber security and privacy protection as global challenges. The (potential) role of an EU–U.S. partnership on this issue was of greatest interest in this regard. Initially, Sven Herpig, Judith H. Germano, and Philipp S. Krüger provided their perspectives on the topic. The ensuing lively debate concentrated on the cyber technology and insurance market, certification, and the role in Europe of data protection authorities (DPAs), which have an important supervisory function within the legal framework.

The first general question arising from the presentations asked why a U.S. monopoly on cyber technology has developed over the last few decades. As an example, the so-called 'internet big five', consisting of Apple, Google, Microsoft, Amazon and Facebook, are all situated in the U.S. and not in Europe. The participants were divided on this and highlighted different aspects in their answers. One aspect was that European companies initially had a number of problems. German businesses, for example, are predominantly active in the fields of machine-building and chemicals, not the internet technology and services area, and joined the market too late. A further problem for many companies is that research and development (R&D) does not play a central role as it does in the U.S.. Contextual factors have also influenced developments in Europe as economic shocks have hampered innovation and, more generally, market opportunities have been missed. Another emphasis was put on the U.S. consumer market, which for a long time was much broader than the European one and therefore provided more incentives for progress for companies. Furthermore, it has been argued that the concentration of companies in the U.S. might stem from the fact that Silicon Valley is perceived as the 'place to be' and a role model of technological progress, so many companies start or go there.

Besides the reasons for dissimilar market developments, the participants arrived at disparate positions on the issue of why cyber insurance is handled differently in the EU and the U.S.. It was suggested that U.S. companies might be less careful regarding cyber security issues because of the bigger cyber insurance market. However, criticism of this has been expressed as U.S. companies have an interest in taking cyber security seriously because data breaches, for instance, could severely damage a company's reputation. Overall, U.S. insurance handles a lot of development; nevertheless, there are areas where confusion remains. The market itself has been characterised in the debate as not being underwritten since market

failures result in a wrong focus on post-breach actions and measures. Some participants predicted that insurance companies could function as international harmonisers by quantifying risks and thereby assisting companies to better understand and address 'cyber hygiene', cyber security and privacy in an internationally more consistent way. Regarding this, others raised concerns that insurance companies may not always be sure whether a risk is an insurable risk, which is why relying on them might be problematic. In particular, setting benchmarks and defining best practices have been emphasised as important future tasks, particularly with a view to the elaboration of a global framework.

With the focus shifting again onto the U.S.–EU relationship, the work and role of Europe's data protection authorities (DPAs) were subsequently debated. The landmark decision of the European Court of Justice (ECJ) in the Schrems v Data Protection Commissioner case (C 362/14) of October 6 2015, raised important questions for the participants regarding the jurisdiction of national DPAs. In Europe, every Member State has a DPA responsible for data protection supervision. Before the ruling, companies preferred to discuss and settle privacy and data protection issues with the DPA of the Member State in which they had their European headquarters. Some companies, however, engaged in forum shopping by choosing a relatively inactive DPA in any of the countries where they had a branch. One of the core results of the decision was the invalidation of the Safe Harbour Agreement, which had regulated data transfer between the EU and the U.S. since 2000, following the European Commission's safe harbour decision that allowed U.S. companies to transfer data from the EU to the U.S. if they met certain criteria. In addition, however, the powers of DPAs have also been reconsidered in the ruling. Both DPAs and the Commission play a central role in regulating data flows as they have to assess the level of data protection guaranteed in third countries. After the Commission had issued its Adequacy Decision on data transfer to the U.S., the DPAs kept quiet and did not challenge the Commission's decision. In the Schrems case, the Irish Data Protection Commissioner, to whom Maximilian Schrems had turned in his concern about Facebook's transfer of personal data of European users to U.S. servers, rejected the investigation of the case explicitly because of the Commission's Adequacy Decision. Schrems, however, challenged the DPA's decision —first before the Irish court, and afterwards before the ECJ, to which the Irish court referred for a preliminary ruling in the case. In its decision, the ECJ clarified that it is imperative for national supervisory authorities to fulfill their tasks in the European data protection regime by assessing whether a transfer of data to third countries complies with the standards set in the EU and to have complete independence in their decisions. They are, in fact, empowered to decide on the adequacy of the data protection level in a third country, independently of the Commission's decision. Furthermore, the ECJ decided that it is the national DPA's duty to investigate claims brought forward by individuals concerning the adequacy of the level of protection. DPAs in Europe should be included more comprehensively in this process. The decision and effects of the ruling, however, resulted in disagreement among the discussants, especially on the practical consequences for companies. Companies, on the one

hand, would still prefer to interact only with one DPA when problems arise, as approaching every DPA in the EU would take a lot of time and might complicate matters. The European DPAs, on the other hand, emphasise that many of them, if not all, want to be included in the process of finding solutions for data protection problems —an issue which has been solved by the GDPR, which grants the DPAs more powers. Another point of debate was the question of enforcement and whether all DPAs are responsible for enforcing the rules or only a few or one, and, more generally, whether they are centralised or decentralised. As no answer was agreed upon, this aspect calls for further investigation and debate.

In the final part of the discussion, the participants addressed the problems and potentials of certification processes and the development of new technologies in the EU and the U.S.. In this area, once again, different legal traditions influence the development of new products and innovation more generally. One participant pointed out that comparing the U.S. and German approaches, for example, shows that in the U.S. innovation often comes first and the law is considered only afterwards, while the German approach is more cautious, first looking up the law and then initiating new developments.

Concerning cyber security, the discussants saw more opportunities to find a common ground than in the case of privacy and data protection, where the distinct backgrounds would be more obstructive. For ensuring cyber security in product development, mutual standards were thought to be of considerable importance. One way to achieve this is through certification schemes for products. Despite their relevance, the participants outlined several problems regarding certification schemes. As a general issue, the establishment of common standards is often limited as secure devices are not frequently used or as particular agreements of companies and governments stipulate special requirements. For the EU in particular, the position has been expressed that the 'unionisation' of national certification processes could create problems for leading players, especially from Germany or France, because they might lose a competitive advantage against players from Southern European countries that now have lower standards. Nevertheless, some kind of harmonisation to reach an equal level of security by common standards is required. In Europe, a new legal framework on certification is on the way; internationally, the Common Criteria Recognition Agreement (CCRA) is an attempt to overcome the fragmentation of standards. This international framework (ISO/IEC 15408) aims at establishing a situation where products can earn a CCRA computer security certificate which can then be used without further evaluation. Such certificates are issued by authorities of signatory countries, which include numerous European countries, but also the United States. However, there remain problems with this certification, as the participants stressed. The Common Criteria's requirements are considered as currently being too high for CC schemes prevailing on the market across the board. Additionally, its main focus is on evaluating a product's evaluation documentation, which does not directly assess a product's merits, actual security, or technical correctness. Despite the need for further reform, the standards already in place are seen as a first important step towards a common approach to cyber security among states with different practices and backgrounds.

THE REGULATORS' TOOL BOX

Transfers of Personal Data to Third Countries: Certification Mechanisms, Binding Corporate Rules, and Codes of Conduct as Suitable Alternatives to the 'Adequacy Decision'?

MAXIMILIAN VON GRAFENSTEIN

INTRODUCTION: THINKING SUBSTANTIAL REQUIREMENTS AND PROCEDURAL COMPLEXITY TOGETHER

Thank you for the opportunity to speak about the idea of how the co-regulation instruments foreseen under the General Data Protection Regulation (GDPR) could be used, beside the commonly known adequacy decision called 'US Privacy Shield', for the legitimate transfer of personal data to a third country (which means outside the EU). The idea of this presentation stems from my doctoral thesis where I focused on the principle of purpose limitation in data protection laws from the perspective of regulating data-driven innovation. Please bear in mind that the following thoughts are in an ideation phase. This means that I am highly interested in hearing your opinion on whether or not the proposed approach might be a suitable way of solving some of the problems currently being discussed with respect to the US Privacy Shield.

The following two aspects are of particular importance for the following discussion: The first aspect refers to substantial requirements for safeguards that guarantee that the processing of personal data that is transferred to a third country complies with the GDPR. The second aspect refers to the scope of these safeguards, which can have an important impact on the procedural complexity of setting up such safeguards. The main idea of this presentation is that a safeguard with a narrower scope than the US Privacy Shield might be more suitable, at least procedurally, in order to strike a balance between the conflicting interests. To understand this idea, it is helpful to quickly recall the main problem that is being discussed with respect to the Privacy Shield, as well as the co-regulation instruments that can guarantee an equivalent level of protection for the data transfer. In this regard, the following quote from the ECJ case Schrems v Facebook will serve as a starting-point:

> Legislation is **not limited to what is strictly necessary** where it authorises, on a generalised basis, storage of **all the personal data** of all the persons whose data has been transferred from the European Union to the United States **without any differentiation, limitation or exception** being made **in the light of the objective pursued** and without an objective criterion being laid down by which

> to determine the limits of the access of the public authorities to the data, and of its subsequent use, for purposes which are specific, strictly restricted and capable of justifying the interference which both access to that data and its use entail.[1]

On that basis, the ECJ came to the conclusion that the Safe Harbour agreement (which preceded the US Privacy Shield) did not sufficiently restrict state access and was, therefore, null and void. From a European perspective, one of the main questions therefore is whether the new US Privacy Shield now provides a satisfactory answer by sufficiently restricting state access to personal data. (Other problems are whether the Privacy Shield provides for sufficient control mechanisms against unlawful access to the data or not, and whether the assurances given by the former US government are sufficiently robust against the current and future governments).

SUBSTANTIAL REQUIREMENTS: BALANCING THE AMOUNT OF COLLECTED DATA AGAINST THE BROADNESS OF (POSSIBLE) PURPOSES

The requirement to sufficiently restrict state access to personal data stems from the so-called principle of proportionality and, more specifically, the principle of purpose limitation in data protection laws. In the German jurisdiction, both principles are related to each other. Of course, the German Basic Law is not used, at least not directly, to interpret European secondary law, such as the EU Data Protection Directive or the EU General Data Protection Regulation. These laws are interpreted in the light of the European fundamental rights to private life under Art. 7 ECFR and data protection under Art. 8 ECFR. Even if the interplay of both fundamental rights is not yet clarified, it is clear that these fundamental rights do not equal the German basic right to informational self-determination but provide for a conceptually autonomous concept of protection. However, in the European legal system, it is commonly accepted that the different Constitutional Courts on the Member-State and European levels cultivate a behaviour that is described as a 'co-operation between the various fundamental rights regimes' (in German, 'Grundrechtskooperation'). In particular, European primary law contains several provisions that formally reflect this idea, such as Art. 6 sect. 2 TEU referring to the constitutional traditions of the EU Member States, or Art. 52 sect. 2 ECFR referring to the European Convention of Human Rights. But also, on a more informal level, one can observe that Constitutional Courts refer, more implicitly than explicitly, to other constitutional regimes using them, at least as a source of inspiration. One example where this can be observed particularly well is the ECJ data retention case Digital Rights v Ireland (ECJ C-293/12), on which the Schrems case was widely based. The Digital Rights decision from 2014 takes up the reasoning, on an almost literal basis, by the German Constitutional Court in its case

[1] ECJ C-362/14, cip. 93; the bold sections have been highlighted by the present author.

decided in 2010 (and where it referred to the German right to self-determination, even if the German law in question was actually based on the European data retention directive). Given the extensive and detailed case law which the German court has provided over the last three decades in this regard, and its potential pace-making function for future ECJ decisions, it can be helpful to take a closer look at how the German court answers the question of how to sufficiently restrict state access to personal data.

There are two moments where the assessment of whether a state's data processing meets the principle of proportionality must be carried out. The first moment is the moment of data collection. The second moment is when the collected data is (re-) used at a later stage. In general, there are four criteria guiding the assessment. First of all, the principle of purpose limitation, as well as transparency, data security, and additional controls. Transparency and controls can be important criteria, in particular, with respect to intelligence agencies. An important question in this regard is how to provide transparency if the agencies act secretly. In Germany, this lack of transparency is usually re-balanced by controls through an enquête commission. It would be interesting to compare these mechanisms more precisely with the US situation. Maybe both kinds of controls are not so different to each other as it seems. However, in this discussion we are focusing on the principle of purpose limitation. As far as the moment of data collection is concerned, the principle of purpose limitation requires a balancing exercise examining how broadly or narrowly a processing purpose is specified: the broader the purpose, the more probable it is that the collected data is also used for purposes which are intensive (i.e. which conflict with the fundamental rights of the data subject in an intensive manner). If there is a broad and/or intensive purpose, then the data controller must restrict the amount of collected data and/or collect only those types of data that are not very sensitive for the data subject. For instance, personal data collected in public is considered less sensitive than data collected in somebody's home. Another criterion is the reason why the data is collected. The court considers a danger that is only abstract always insufficient for the collection of personal data. Instead, the danger has to be specific. This means that there must be certain circumstances allowing the conclusion that a certain action leads, with a sufficient degree of probability, to harm for a specific object of protection.

Let me illustrate this with an example. Applying this balancing exercise, the German Constitutional Court has come to the conclusion that the collection of a large amount of personal data for intelligence service purposes can be legitimate because this purpose is not intensive. The reason for this is that this kind of data is only used to inform the German government. Instead, the collection of personal data for criminal investigation purposes is much more intensive for the individual because he or she could be imprisoned as a result. Therefore, the criminal prosecutor is allowed to collect only a small amount of personal data for such an intensive purpose.

Regarding the second moment where the proportionality assessment becomes relevant, that is to say, the later (re-)use of the data, in its recent decision Federal Criminal Police Office Law ("BKA-Gesetz")[2], the German Constitutional Court has provided for an important liberalisation of its understanding of the principle of purpose limitation: First of all, the Court states that there is only a (re-)use of the collected data for another purpose than that originally specified within the law if the processing pursues the protection of another object of protection than that originally referred to. For example, if the data was collected to protect human life, this data can be used on the same legal basis if the controller is still the same authority and the purpose protects the same object of protection as indicated previously. Even if there is another purpose, another liberalisation applies that is called the 'hypothetical collection test'. This test requires the data controller to ask the following question: Would I be allowed to collect the data for the same purpose that I would like to re-use it for now? If the answer is yes — that is, if the controller was allowed to newly collect the data for the new purpose, then it could also re-use the data for that purpose even if it was collected for another purpose. Actually, this test is not really a liberalisation of the principle of purpose limitation but already rather old. This so-called 'hypothetical collection test' stems from the preceding cases Surveillance of Telecommunications I[3] and Usage Ban Regarding Surveillance of the Home (Verwertungsverbot Wohnraumüberwachung)[4]. In that case the German intelligence service collected a large amount of telecommunication data for the purpose of providing information to the government. This was deemed legitimate (see above). However, within these data sets, the intelligence service discovered data which could have been used for the prosecution of specific crimes. This was a re-use of the data for another purpose. The Court considered this re-use legitimate as long as the intelligence service made sure that only this kind of data was given to the prosecutor. Thus, the prosecutor was not allowed to have access to all the collected data, but the system had to be organised in such a way that the transfer of the data was restricted to an extent where it could be considered proportionate pursuant to the new purpose.

This description hopefully gives a sufficiently accurate impression about what is, or more precisely, what may be meant by the legal requirement to 'sufficiently restrict state access to personal data'.

[2] Judgment of 20 April 2016, 1 BvR 966/09, 1 BvR 1140/09).

[3] (Telekommunikationsüberwachung I, Order of 14 July 1999, 1 BvR 2226/94)

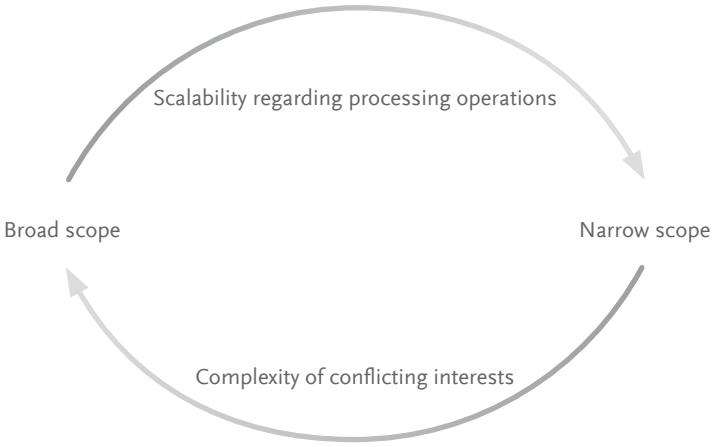
[4] Order of 7 December 2011, 2 BvR 2500/09, 2 BvR 1857/10).

COMPLEXITY VS. SCALABILITY: CHOOSING THE APPROPRIATE SAFEGUARD PURSUANT TO ITS SCOPE

Now, let us shift our attention from these substantial requirements to the procedural aspect mentioned at the beginning: the scope of the regulation instruments that safeguard an appropriate level of protection if the data is transferred to a third country outside the EU. Art. 44 et seq. GDPR list several means by which data controllers or processors may guarantee sufficient restriction of state access to personal data transferred to a third country. An already known means is the so-called 'standard contractual clauses'. However, there are also further means, namely binding corporate rules, approved codes of conduct and certification mechanisms. The aspect that makes them interesting with respect to the procedural complexity of setting them up is their different scopes: While binding corporate rules refer to the processing activities of a group of undertakings, a code of conduct covers the processing activities within a processing sector, and a certification mechanism refers to a single processing activity, or at least several processing activities on which a single product or service is based. In any case, the scope of these co-regulation instruments is narrower than that of an adequacy decision, which principally covers all kinds of processing activities of all kinds of data by all kinds of controllers and processors.

So, why does the scope matter? There are two reasons for this assumption. First, because when negotiating an adequacy decision, such as the Privacy Shield, there are many more different interests involved, which makes it more difficult to find a solution that fits all the conflicting interests. In contrast, a narrower scope, such as that of a certification mechanism, implies less conflicting interests. Given the extremely broad scope of an adequacy decision, this may well be a reason why the US Privacy Shield might never reach a level where it satisfies all European and North American interests. Indeed, what makes an adequacy decision interesting is its scalability. An adequacy decision covers all sorts of processing activities. Thus, the more data controllers and processors can base their processing activities on this regulation instrument, the better it 'scales'. However, if this scalability results in the instrument becoming too complex to set up, it might make sense to narrow down the scope. The second reason is related to the principle of proportionality, as explained before. If an adequacy decision covers all sorts of purposes, from very narrow and less intensive purposes to very broad and intensive ones, one has to re-balance this intensity by increasing the transparency, enforcing the controls and restricting the data base. Binding corporate rules, codes of conduct and certification mechanisms can define, precisely, all three 're-balancing' mechanisms. In particular, the amount of the data transferred is limited to the characteristic nature of each of these co-regulation instruments. For example, a certification mechanism could well focus on just one single set of personal data —which may, however, be an economically important one— and define for which purpose and under which conditions this kind of data could be transferred. These limitations make the setting up of such an instrument far less complex than an adequacy decision. The following chart my illustrate this thought:

Scope = Scalability vs. Complexity



CONCLUSION: ASSESSING MORE PRECISELY THE ROOM FOR MANOEUVRE

In conclusion, what we could do is to (1) examine precisely the room for manoeuvre left by the case law of the ECJ, taking the case law of the constitutional courts of other EU Member States into account; (2) examine for which purposes personal data will certainly be processed by state agencies if transferred, for instance, to the USA; (3) and then determine which kind of data can be transferred under which conditions, proportionately given these purposes. Thus, we cannot simply change US law, nor can we change the case law of the ECJ, but we can make legal analysis preciser than it has been, and we can define what data is transferred and under which conditions much more precisely than in the US Privacy Shield.

Normative Instruments for Private and Secure Transatlantic Data Flows: Cyber Insurance and Liability Localisation

TYSON BARKER

I am going to approach this topic from a couple of different angles. First of all, it will not be a legal angle necessarily, but more an anthropological angle. Second, my focus is not exclusively on data, personal data or data breaches per se but rather on operational technology and the development of liability localisation as it relates to critical infrastructures. This presentation is largely based on research that I did with Tim Stuchtey at the Brandenburg Institute for Society and Security. So I am going to talk about cyber insurance today, and about liability localisation in the United States and a little bit in Germany, and throw some shrimp on the barbie and see if it provides some input for discussion.

At first, I want to focus on the idea of nudging. This is the idea brought forward by Cass Sunstein as well as Richard Thaler —who just won the Nobel Prize— of creating indirect incentive structures that lead to voluntary compliance with expected behaviour. I think that when you are creating liability and you are shifting it and you are kind of manipulating it, that is one example of nudging. Some people might say, 'What has that got to do with liability? That is something legal'. But the truth is that in a lot of areas, as we will see, cyber liability —the history of liability, for example, in personal data— is relatively new, and has some interesting aspects worth pointing out in the history of risk management the United States, but probably also in Germany.

So why insurance? Of course, insurance is the way we deal with risk, the way we hedge risk. One area of potential of this regulatory instrument is that it can drive innovation and standard setting in all sorts of areas. A primary example of this is the support for the automatic fire sprinkler. This was originally developed by an American who could not get a factory to buy his sprinklers. He noticed, however, that factory owners were starting to be insured or they were creating mutual insurance schemes. He and others pushed for the adoption of sprinklers and incentivising their use through lower insurance premiums. So the entire adoption of this new technology —of course, fire is a static threat as opposed to cyber threats, which can be dynamic— nevertheless shows that schemes can be created that incentivise the adoption of a risk-mitigating behaviour through insurance. It is interesting that in the area of fire and also in the area of automobiles, it was insurance that for a long time drove the development of standard-setting and specifications.

The next question is: how does cyber insurance look in the United States, what does the market look like? This part will focus on data breaches in particular. Online data protection in the United States has pretty discreet origins and pretty specific pieces of law: HIPAA, regulation for financial data, and of course state-based data protection schemes. And these state-based data protection schemes started to create a market for insurance or hedging, and these insurance schemes cover a lot of things. First of all, they cover legal costs, reputational damage in cases of business interruption, and first- and third-party general damage. As can be seen, this describes the beginnings of cyber insurance in the United States. After 9/11, and this relates to the operational technology side effects and critical infrastructure side effects, there was a fear in the insurance market that there could be a 'cyber 9/11' or terrorist acts in general that would be so costly that it would lead to the collapse of the insurance market. In the United States, the government said that if such cases occur —the term 'cyber 9/11' was heard a lot in that debate— the US government will be the reinsurer of last resort. The government said that it will cover amounts over a hundred million dollars, and that has been reaffirmed recently in national cyber insurance policies, I think this was stated by the Treasury Department just at the beginning of 2017.

In the Homeland Security Act, US law makers also included a provision known as the Safety Act, which is the scheme for certification by the Department of Homeland Security. It says that they will certify certain technologies, certain patches, and designate them as Safety Act-compliant. If these technologies can then be used in IT operators —for example in factories or power plants— and something occurs, the risks will be transferred to the company that is certified and through that to the government. So this means they are playing with the liabilities exemption scheme in order to encourage the adoption of these technologies. Basically, the government says that if someone adopts these technologies, the government will assume all the risks associated with it. But this has been slow to catch on.

And then, of course, in the United States we have the definitions of what critical infrastructure is and we have started to get frameworks for general norms in this cyber security framework. In this area, a dialogue on the insurance process itself has started: How can insurers encourage critical infrastructure or, more generally, clients, to adopt cybersecurity frameworks? This is a question that the U.S. has been dealing with pretty intensively since about 2014, and the government body that has been dealing with this is the Department of Homeland Security. The reason why they say they want to deal with it is because they do not have any kind of legal authority to do so. They do not have the intelligence service's legal authority to extract information from companies, and they do not have the Treasury Department's legal authority to levy fines and impose computer regulations. Therefore, they have been seen as honest brokers. DHS has led the effort to establish greater information sharing based on risk within and between sectors. The effort has been slow moving but shown some signs of progress.

The core cyber insurance market in the United States is relatively large compared to other countries. The total value of premiums for cyber insurance is approximately between two billion and three billion U.S. dollars, and the biggest payout capacities are about 250 million. I think the biggest on-record payouts were in the Target incident that happened two years ago. There are more than 500 offerings, and some of these are offerings in general liability for general property insurance. Furthermore, there has been a lot of playing with exemptions in those policies themselves. Some of them are stand-alone policies, particularly in the area of data protection. It is clear that the threats are changing for industrial control systems in critical infrastructure. It is interesting to note that it used to be energy attacks on power plants that were the primary threats. Now it is more in manufacturing —I think this is probably similar to what is happening in Germany.

Overall, there are unique aspects of the insurance market in the United States, and the question is: would it have lessons for Germany and the transatlantic relationship? The U.S. is obviously the first mover in this area, and U.S. states play an enormous role in the regulation of insurance and in the regulation of data breaches and data protection, which can be seen from the laws of California on personal data. There is a much more litigious legal culture, and there are also class action lawsuits which have also driven insurance market development. There is a focus on voluntary compliance and information exchanges. The government's work has focused on positive incentives, either through the reinsurance model, through data liability exemptions, like the Safety Act, or through its convenient role, like the Department of Homeland Security. Moreover, there are more and more collaborations between insurers and cyber security service providers in Silicon Valley who are saying, 'What kind of alliance can you set up whereby if somebody adopts our technology and our consultation, it will lower premiums?'

In Germany, the picture is quite different. As a starting-point, the size of the market is much smaller in Germany, where total premiums amount to just over 20 million dollars —so 20 million vs two to three billion dollars. The United States is really the place where cyber liability and cyber insurance were established as an instrument to handle cyber risk, and has really taken hold. The German market is immensely underdeveloped in this regard. What could lead to changes in this area are the IT security law or the GDPR, although the legal structure still does not allow for personal damages in the form of class action lawsuits. So you don't have individuals driving this process in data breaches, looking for restitution for data processed in Germany, like in the United States. Usually, at least in the United States but also in the UK, there has been a wake up call moment. The Deutsche Telekom router incident could be one of these events. It has changed some thinking, and at least in the critical infrastructure area, and for industrial control systems it was the German steel mill cyber attack from late 2014. But we still have not seen this big emphasis on the cyber insurance market.

Finally, what are the global trends in cyber insurance? It's a growing market: it is said that it will be worth about 7.5 billion dollars in global premiums by 2020. Institutions like Lloyd's of London are thinking about cyber insurance offerings for their clients. So what is the integrated systems environment for power plants, for banking systems, for supply chains —what happens if things are knocked out? And because of that there is a lot of attention focused now on business interruptions in supply chains, more so than was the case five years ago. There is some big profit for ransomware, and Wannacry proved that last year about ten percent of claims for data breaches were related to ransomware, and this year it is already up to 25 percent, especially in Asia.

In addition, there is a movement away from solely data breach or even critical infrastructure environments to talk more about operational technology, and more specifically the internet of things, and this is an interesting area. I think we will have implications for Germany —the world's automaker. There changes are appearing. Obviously, regarding an auto, we are all part of the insurance, but as self-driving cars as smart vehicles are starting to be developed, the companies that are producing them are trying to think about how they should assume that responsibility. With that they are going to see some of the standard-setting and update responsibility for those people's vehicles— in all these things we could see shifts and where liability is localised. Consequently, the idea of liability swinging, liability localisation exemptions is something that I think we should talk about when we talk about cyber regulation.

Discussion: Normative Instruments for Private and Secure Transatlantic Data Flows

MARIE-CHRISTINE DÄHN

The third session of the workshop focused on the set of legal and non-legal instruments available to legislators. In the first block of the session Maximilian von Grafenstein, Christopher Kuner, and Tyson Barker reflected upon the normative instruments for private and secure transatlantic data flows. In the subsequent debate, attention focused on the legal contexts and consequences.

The two core points of the discussion were the current fragmentation of the legal framework governing data protection and the need for dialogue not only between jurisdictions but also between courts at all levels. In the debate, the legal fragmentation was seen as a result (or a product) of privacy and data protection being particularly culturally sensitive. This means that different states or regions have different approaches to and perceptions of the requirements of data protection. On the one hand, this had already become apparent in the earlier discussion on T. Christakis and R. Milch's presentation comparing the European and U.S. legal traditions regarding privacy and data protection; on the other hand, a great diversity of national data protection traditions shaped and fragmented European law for a long time. One of the main aims of the General Data Protection Regulation (GDPR) is the harmonisation of data protection law throughout the Union, since under Directive 95/46/EC, every Member State transposed the overall goals of the directive into national law its own way so that a patchwork of data protection levels emerged. For the EU, the U.S., and the global level as well, the participants widely agreed that fractured rules are not only costly but also reinforce legal uncertainty and impede effective enforcement. The GDPR could be seen as a benchmark or blueprint for others to follow. Nevertheless, there was disagreement on the enforcement of the fines the GDPR imposes as sanctions if the data protection rules are violated (Art. 83 Secs. 4, 5, 6). Some raised the concern that sanctions could too easily be avoided while others pointed out that this concern is unfounded as the GDPR has sufficient mechanisms to ensure that fines cannot be averted if there is non-compliance.

One aspect that has a decisive influence on the development of the legal framework is the work of the courts. These, however, do not always act in concert. It has been remarked that when comparing the rulings of the European Court of Justice (ECJ), the U.S. courts or the German courts, the same body of law could be interpreted in multiple ways. Some of the participants in this regard characterised the current developments as indicating a call for the synthesis of European jurisdictions. In this, the ECJ as well as the European Court of Human Rights (ECtHR) nonetheless consider national-level legislations and decisions. Participants

noted that talking about a competition of protection levels is not appropriate since recently as there seems to have been a move towards greater cooperation in general. Another facet of bringing jurisprudence closer together is the concept of the 'dialogue of the judges' which one participant introduced into the discussion. In the EU, it describes both, a formal procedure of references by national courts to the ECJ seeking common interpretation, and an informal process where single European constitutional courts monitor what other constitutional courts in the EU are doing. In particular, this includes tracing other courts' rulings and referring to them —not necessarily directly by quoting them but more through considering them and bearing them in mind as a background. This might advance common understandings as mentioned above. While the judicial dialogue under Article 267 TFEU is binding, constitutional courts are not obliged to practice the informal interchange, especially as different legal traditions can impede it, but it is considered as a way of enriching their work and may lead to a more coherent legal practice.

Despite the ongoing convergence of (constitutional) law on both sides of the Atlantic, the question that remained for the discussants was how global standards could be developed. Although it became clear that there is a general need for global approaches, it was remarked that these will not emerge rapidly. A global regulatory framework requires time to be developed. As one participant argued, it will come, but cannot be forced at once. Regarding this, the relevance of different contexts plays an equally important role in both the European and U.S. legal environments: manifold traditions and understandings influence the kind of approach that will be pursued. Some, for instance, may strive for a direct legal regulation while others prefer binding corporate rules or other forms of self-regulation or regulated self-regulation.

The current EU and U.S. approaches to cyber security may illustrate such differences. While the Union tackles the issues in this regard through the GDPR and the Directive on Security of Network and Information Systems (NIS Directive) with strict breach notification and security requirements which lead to the European approach being characterised as 'formalistic', the U.S. administration puts the focus on addressing national cyber threats and cyber security in the IoT and for critical infrastructures, although both perspectives are not mutually exclusive. Consequently and additionally, the progress in achieving effective protection and security might differ between policy areas, e.g. legislators may agree upon rules for cyber security, but still do not reach an agreement for a global data protection framework. In order to find common solutions, one participant emphasised that players should refrain from being too assertive in promoting their own approaches as legal imperialism may undermine the legitimacy of the solution. The EU, for instance, transposes its system of equivalence in data protection to other countries when data is transferred to third countries. Such a process, however, takes place in various fields of law in different countries. Especially if influential actors set a certain standard, it can evolve into a model for others. This can become problematic when the actors only accept another actor's regulations if they adopt the latter's approach. Therefore, finding a common ground on one issue could improve mutual understanding and thereby enhance the chances of finding solutions for problems in other areas.

Procedural, Institutional, Technical and Management Devices: A U.S. Perspective

IRA RUBINSTEIN

I am going to try to be a bit more concrete in my remarks but I will begin with a broad question, which is: how alike are privacy and security? We discussed this a little bit yesterday. I think the similarities were overemphasised but there are important differences, too. One difference is that privacy, far more than security, is a normative concept and a contested concept. Like Derek Bambauer, I think of security in broad terms as implementing privacy choices once normative issues have been settled. For example, if privacy requires limited access to data, limited to certain persons, security is the means to provide such access and ensure the privacy outcome. That is one difference. The second difference is that because privacy is a more contested concept than security, one can readily imagine alleged privacy violations where someone takes the contrary view and argues that these supposed privacy violations in fact promote social goods. There are many such examples from the big data setting where these sorts of disputes might arise. Security does not have these characteristics —security violations are just 'bad' and there is really no associated social good.

I want to talk now about how these differences play out in two provisions of the GDPR: Article 25 (data protection by design and default) versus Article 32 (security of processing), which may easily be understood in terms of 'security by design'. I have spent some time looking closely at these texts and trying to outline how they differ. It seems to me there are two broad questions about Article 25 on data protection by design and default. One is: what does it require companies to do? It is clearly a compliance obligation but as I look at the GDPR overall, it has general principles, provisions identifying a data subject's rights, general obligations of controllers and processors, and administrative provisions. What is it that Article 25 adds? How do you know as a controller or processor when you are compliant with Article 25, assuming that you are in compliance with these remaining provisions? What do you really need to do to satisfy Article 25? That is an internal perspective, but I also want to take a more external perspective by seeing how Article 25 interacts with the broader literature on privacy by design. This is analogous to how Article 32 interacts with the broader security literature, some of which we have already discussed. The second question that I want to raise has more to do with this external perspective. It asks: what conception of privacy by design is presupposed by the regulators in Article 25? Because there are in fact many different models of privacy by design and it is not at all clear which conception the regulation builds from.

So, let us discuss the first question: what does Article 25 do, what does it add to the obligations otherwise existing under the GDPR? It is clearly a provision designed to allow controllers and processors to demonstrate compliance. In this sense, it is similar to a number of other provisions like BCRs, model contracts, codes of conduct, and certification mechanisms. What is different about it, I suppose, is that it focuses on technical and organisational matters —one of the key phrases in this article is that controllers 'shall implement... technical and organisational measures'. But what do these measures consist of? And also, what default is required?

Well, the text imparts several clues. We know who it applies to —to controllers and processors— and we know what they have to do: implement appropriate technical and organisational measures which are 'designed to implement data-protection principles'. I would submit that this is not very illuminating, which reinforces what I would call the self-referential quality of Article 25: it is all about compliance, but firms are already required to do all these other things in order to comply with the GDPR, so what more should they do? There is kind of a belt and suspenders aspect in Article 25. You have already taken many compliance steps, but now you have to do this additional thing involving data protection by design and default. Article 25 advises firms to take account of the state of the art, costs, the nature and purpose of the processing, and the relevant risks and then implement technical and organisational measures —this is somewhat helpful. Some examples are provided, such as pseudonymisation, data minimisation, and encryption. And firms are also instructed as to timing: these measures are required both before and during processing. But even though firms know this, I would submit that there is still much that they do not know. So, I still have a few questions.

The most fundamental question is whether it is a violation of Article 25 not to use any of those technologies that are given as examples? In other words, are data minimisation, pseudonymisation and encryption always necessary? And is it always necessary to use all three of them? What if the controller or processor argues that in a given case they are not especially helpful? Supposing they decide not to implement them, is it still possible for them to comply with Article 25? Again, how do they know that they are in compliance or not? We could look at the relevant recitals (number 78), but I do not find them very helpful —they still have this kind of self-referential quality. Or we could stay with this internal perspective, and compare Article 25 with some other GDPR provisions that bear upon 'technical and organisational measures' —I will just quickly mention a few.

To begin with, Article 25 resembles very closely the general obligation under Article 24 concerning 'responsibility for the controller' —in fact, the language is almost identical, with the exception that Article 24 also requires the implementation of 'data protection policies', whereas Article 25 only references technical organisational measures. Again, that does not tell us very much. Article 25 also very closely resembles Article 32.1, which requires roughly the same methodology, though somewhat different goals. Confusingly,

however, some of the examples of technical or organisational measures in Article 32.1 include 'the pseudonymisation and encryption of personal data'. Are these security measures, or are they data protection measures? One way in which the two articles differ is in terms of their goals. The goals for Article 32, for security by design, are easier to define very precisely because they have meaning outside the sphere of the GDPR, that is, we can reference external security standards that frame the well-known CIA triad of confidentiality, integrity and availability. These standards have been around in the security field for decades, they are well developed and firms understand what they mean and how to achieve them. I would submit that there is really nothing comparable in the privacy by design setting that would provide that kind of guidance and tell organisations what they need to do; instead, organisations are just told that they need to meet the requirements of the GDPR by implementing these mechanisms which are designed to implement the GDPR. And this seems very circular.

And then, finally, there is some conceptual overlap between Article 25 and the privacy impact assessments (PIAs) required by Article 35. I think this is a much better drafted provision: it is clear what triggers a PIA —high risk— and it is also clear, thanks to a recent working party guidelines document, what the criteria are for high-risk processing. But none of this is similarly available under Article 25.

I want to just quickly mention the default provision of Article 25 and then I will try to draw a few conclusions. The default provision is a bit clearer because it gives some examples of default measures limiting the quantity of data collected, the period of storage, and their accessibility. One can think of some simple examples of this, such as the fact that apps should not process location data if such data are not needed, and should not use pre-checked checkboxes, or ask for sensitive patient information if it is not really needed, but I think in more complex cases, I am not really sure I could implement those provisions. Take, for example, Facebook's news feed feature. Under this default provision, should Facebook not draw on all the data it has regarding an individual, using its algorithm to decide what to put in the news feed? Should it throw away some of that data despite the fact that the 'Timeline' covers an extensive period (one's entire life)? I do not think the answers to these questions are clear.

So, let me turn to the external perspective. I think that externally to the GDPR security provisions, there are security standards recognised by ISO, ENISA, NIST and so on; there is the recent European cyber security certification framework; whereas even if one thinks of PIA requirements as referencing external standards, they differ by nation. And, in any case, there is nothing quite like this in the privacy by design space, and I think, part of the reason for this is that there are multiple models of privacy by design, none of which are dominant in terms of regulators endorsing them.

I can identify at least five models of privacy by design: The first is just the basic life cycle process that you have built privacy in, and you have to do it in the design and development, you have to do it in the implementation —so the emphasis is on stages of design. The second is more of an accountability mechanism and resembles PIAs. A third is adopting specific engineering techniques, and the GDPR seems to embrace this to some extent by identifying a few sample techniques (data minimisation, pseudonymisation, encryption) but other engineering techniques are not identified. Fourth, one can think more in terms of specific design (as opposed to engineering) techniques. I have written about this before, and pointed out that an irony of 'privacy by design' is that nobody talks about design. It is actually a discipline of design. For example, the little encryption lock icon used with SSL —that is good design. You see the lock, you know that your session is encrypted. On the other hand, if anybody tries to read a PKI certificate when you get a notice that your certificate is invalid, that is a terrible design. No one has the faintest idea what it means, or what to do about these security 'warnings'. So, design itself is another possible model here. And then, finally, there are privacy-enhancing technologies, or PETs. Of course, PETs come in several varieties: there are 'hard' PETs, which offer privacy guarantees based on crypto-techniques, differential privacy, zero-knowledge proofs, etc. And then there are 'soft' PETs, which offer no guarantees at all, and really boil down to privacy-friendly features (like a dashboard for setting advertising preferences). Again, it is not clear which model the GDPR has in mind.

So, let me try to draw just a few straightforward conclusions from these remarks. First of all, I think that it is important to keep in mind that privacy and security are not the same. Secondly, that the technical and organisational methods for ensuring security are much clearer than those for ensuring privacy, partly because of the contested nature of privacy, and partly because security techniques have been around a lot longer and are much more mature. Third, I think that Article 25 is not self-explanatory and that without additional guidance clarifying what technical and organisational measures and methods mean, this provision just will not serve much purpose —it will be either hortatory or an additional basis for imposing penalties but without any clarity about what steps a controller or processor should take to ensure compliance and avoid violations. Finally, I would point out that, in line with the broader theme of this conference, technical and organisational measures transcend U.S.-EU cultural and legal differences. So, I think it is a very promising area to develop —provided that you can clarify what it means and reach an agreement on which engineering and design techniques are appropriate in which scenarios.

'... on the ground: an industry perspective'

KLAUS LENSSEN

Cybersecurity has become a major challenge for industry. Discussing the topic can be quite difficult due to the various viewpoints and perspectives participants may have. I would like to explain Cisco's approach to cyber security.

With cyber threats escalating, security has emerged as a critical business need and competitive differentiator. Organisations that successfully embed security throughout their network infrastructure, policies, processes, and culture are able to reduce risk while creating sustainable business advantages. Every day at Cisco, we protect our enterprise by securing the 120,000+ people working in 170 countries around the globe and the IT infrastructure they rely on. Our network spans across more than 40,000 routers, serving approximately 26,000 remote office connections and 1,350 engineering labs. Beside 2,500 IT applications, we utilise around 500 cloud applications. These complex data systems produce 47 TB of traffic, 15 B netflow records, 4.8 B DNS queries, and 75 M web transactions —every single day.

Cybersecurity is our top priority. From product development to operations to data protection, we are embedding security everywhere. This pervasive security mindset gives us the power to identify and pivot on issues faster and with greater confidence than ever before. Our commitment to invest across people, processes, technology and policies is helping us build a secure enterprise.

The EU General Data Protection Regulation (GDPR) replaces the existing patchwork of EU National Data Protection legislation and brings a degree of long-anticipated consistency to the data protection landscape in Europe. Essentially, the GDPR from a legal perspective embodies the well-recognised privacy principles of transparency, fairness, and accountability. The GDPR also attempts to introduce a risk-based approach that enables innovation and participation in the global digital economy while respecting individual rights. It also comes with substantial fines (up to four percent of revenue) and other penalties. But the benefits of good data privacy processes extend well beyond avoiding these fines and penalties. Having good privacy is essentially a commitment to our customers.

In our view, the digital economy can only flourish when you connect people, processes, data and things in an ethical, meaningful and secure way. That includes creating an environment in which everyone can easily do business and know their data and privacy is safeguarded. We are committed to helping our customers and partners by protecting and respecting personal data, no matter where it is from or where it flows.

Privacy is an integral part of the digital transformation wave. As more countries, companies and organisations take advantage of cloud, mobile and data analytics, privacy plays an increasingly important role in critical decision-making, product design and service offerings. Innovators who are emphasising privacy as an integral part of the product life cycle are on the right track.

Cybersecurity is the point where it all comes together —data privacy and data security. They are tightly related and inseparable. Data privacy depends on data security, which depends on IT-security, which is part of cybersecurity.

Many organisations around the globe find themselves dealing with infected computers in their environments that are compromised with malicious software. This is happening regardless of the type of organisation or individual; be it a small or medium-sized business around the corner with little or no specialised IT staff, large enterprises, individual citizens, research institutions, NGOs, or even government agencies. The most recent large-scale incidents revealed another dimension of the problem; the impact of ransomware went beyond being commercial. Last year we saw hospitals being held hostage to ransomware, bringing down larger parts of their IT and thus impacting the safety of medical operations. Regular clinic procedures came almost to a complete standstill. Paper-based contingency processes were too slow and cumbersome, with the result that surgeries were postponed so as not to threaten patients' lives. Cybersecurity got a safety dimension.

While experts continue to investigate the technical details, one would think that the most urgent need is to identify and ignite change that aims to lower the chances of this happening again. But there is the flip side of the medal. Governments are afraid of losing ground through their decreasing ability to lawfully intercept and examine evidence at rest on devices and evidence in motion across communication networks, which is described as 'going dark'. Thus, they are striving to foster national security, improve law enforcement capabilities and intelligence services in the digital age, resulting in a different approach, which is what one would expect in the light of the recent cybersecurity incidents. They should prompt a broader discussion about the crucial role that all involved parties play, including those who find vulnerabilities, technology vendors who fix them in products and services, and customers who operationalise technology and rely upon it in this digital age. The approach for each group that contributes to the end result is very different.

A WAY OF THINKING ABOUT THE EVOLUTION OF CYBERSECURITY INCIDENTS

The recent events bring into focus the issues that need to be discussed and thought through when a/an:

– vulnerability is found;
– exploit is created and/or used to leverage the vulnerability;
– technology vendor learns of the vulnerability and issues a fix (or is not aware of an issue);
– technology operator must update (e.g. a customer's IT department).

THOSE WHO FIND VULNERABILITIES

The recent events are a call to action regarding policy changes that put defence and resilience first. We at Cisco plan to amplify the demand for clear policies related to governments around the world disclosing vulnerabilities. Confidence in the global internet is being undermined by allegations that some governments stockpile and exploit security vulnerabilities in products, rather than reporting them to those who can fix them. Vulnerabilities should be disclosed immediately when found, apart from short-term exceptions by court order when an effort to save lives is directly involved. As the shutdown of hospitals in Germany and the UK due to ransomware shows, lives are also put at risk when critical infrastructure is endangered because of undisclosed vulnerabilities.

The recent events underscore the importance of having transparent processes, subject to meaningful oversight, for how governments handle and disclose vulnerabilities. Cisco is, therefore, encouraged to see new bipartisan legislation being introduced in the United States Senate on this topic. We look forward to working with the proponents of this legislation, and with governments around the world to establish new rules of the road. Rules that are designed to quickly route information about vulnerabilities to organisations capable of acting upon it to protect security in a timely manner.

Increased transparency about the process and how it works will build more trust and will mitigate the risks of undisclosed vulnerabilities. It should not be a matter of 'if' governments are required to notify vendors, but of 'how long' it is until governments must notify them. Recent experience demonstrates that we must assume secrets will eventually fall into the hands of those who can exploit them. Therefore, we have to act quickly to ensure vendors have a reasonable opportunity to defend their customers and users before those disclosures occur.

THOSE WHO EXPLOIT VULNERABILITIES

To be clear, those affected by these incidents are victims of criminal attacks. The perpetrators are at fault here. And the affected individuals and organisations deserve a thorough investigation to find the bad actors, and to seek justice as well as peace of mind. To that end, we at Cisco will redouble our efforts to aid law enforcement agencies in identifying the bad actors behind these types of incidents.

THOSE WHO CAN FIX VULNERABILITIES

We must acknowledge and (frustratingly) accept that software, hardware, and services vulnerabilities exist today and will continue to be discovered, no matter how hard we all work to avoid them. With millions of lines of code plus thousands of configuration options, and the ability of a single wrong keystroke to result in a bug that is not detected, complexity is quite possibly the single biggest contributing factor. That said, technology vendors do not get a 'pass' here.

When it comes to managing vulnerabilities and bugs, technology companies' interests and those of our customers need to be 100 percent aligned. Cisco recognises the technology vendor's role in protecting our customers, and we will not shy away from our responsibility to constantly strive to do better. For a decade, we have aimed to reduce the security vulnerabilities and risks associated with our products through industry-leading efforts such as Trustworthy Systems initiatives, the Cisco Secure Development Lifecycle, Cisco Common Crypto models, the Product Security Incident Response Team (PSIRT), and Vulnerability Disclosure policies. Is it perfect? No. Are we ever satisfied? No. Are we striving to do better? Resoundingly, yes!

THOSE THAT NEED TO DEPLOY THE FIXES TO VULNERABILITIES

If you accept the premise that there will be vulnerabilities despite all attempts to avoid them, then once the security update is available, oftentimes it falls to the users or administrators of that technology to deploy it.

Good technology operational hygiene is essential, and organisations need a measurable operational model to understand and manage security updates. This includes having an emergency response process to handle real-time threats like the one we have seen recently. In terms of establishing what is possible, organisations can take into account things like Vulnerability Dwell Times, and the acceptable level of risk within the network —all of which should be understood and agreed to by senior leaders.

Network defence continues to require an ongoing 'protect, detect, and remediate' strategy, and the best way to secure a network is through a multi-layered, end-to-end approach. This means: prevent as many threats as possible from getting in, have tools in place that identify those that do, and others that will contain and fix the issue.

Delivering trust and security in technology is a multi-party responsibility. Cisco remains committed to our holistic security approach beginning when a Cisco product is conceived, through its development, manufacture, and deployment. We will continue to provide the necessary resources so that our customers know what they need to do to safeguard against cyber criminals. And we will also continue to advocate and engage the necessary stakeholders to ensure that policies evolve to maintain confidence in the global Internet.

EU Cybersecurity: Roles and Responsibilities

ROTRAUD GITTER

Incidents such as the data breach at the credit reporting company 'Equifax' that recently came to light and impacted more than 143 million people impressively demonstrate that cybersecurity and privacy are not opposites but are both indispensable resources for the success of a digital society.

In a digital society, cybersecurity is a key prerequisite for the life and communication of citizens as well as for the economy and trade in the EU and worldwide. At the same time, cybersecurity is indispensable for maintaining the fabric of our society and governments' capacity to act.

Ensuring freedom and security is a core task of the state, also in cyberspace. This is why EU Member States have the responsibility to actively monitor and respond to the economic and social changes sparked by digital transformation and to shape framework conditions in such a way that our rights and values can also be enforced and applied in the digital world. However, becoming more digital and connected also means that a Member State cannot ensure an appropriate level of cybersecurity alone. Member States must work together in the EU and with their partners.

EU CYBER SECURITY STRATEGY

Therefore, the Cyber Security Strategy of the European Union of February 2013 —a joint communication of the European Commission and the High Representative of the European Union for Foreign Affairs and Security Policy— and the related Council Conclusions were a major step forward in strengthening cybersecurity within Europe.

In recent years, many measures have been implemented within the Cyber Security Strategy's five strategic priorities: strengthening resilience,preventing cyber crime, developing an EU cyber defence policy, fostering industrial and technological innovation and research, and enhancing the EU's international cyberspace policy.

A key legislative project and a central element of the EU CSS was the Directive concerning measures to ensure a high common level of network and information security across the Union (NIS Directive), which entered into force in August 2016.

The NIS Directive provides for building cybersecurity capacities in all Member States and certain companies —notably the operators of so-called 'essential services' in sectors of critical infrastructures. With the NIS Cooperation Group and the CSIRT network, two new bodies were established to enhance the cooperation of the Member States within the EU.

The Cooperation Group has been established in order to support and coordinate the implementation of the NIS directive among the Member States. It is composed of representatives of the Member States, the Commission and ENISA (the European Union Agency for Network and Information Security).

The NIS Directive also establishes a network of national CSIRTs, whose members consist of the national CSIRTs (Computer Security Incident and Response Teams, also known as 'CERTs', Computer Emergency Response Teams) and ENISA. The task of the CSIRT network is to enhance swift and effective operational information-sharing and cooperation between the Member States. The Member States are currently transposing the directive into national law (by May 2018).

EU CYBERSECURITY PACKAGE

Also, on 13 September 2017, the European Commission and the High Representative of the European Union for Foreign Affairs and Security Policy issued a Joint Communication on 'Resilience, Deterrence and Defence: Building strong cybersecurity for the EU', along with a proposal for several initiatives. This 'Cybersecurity Package' builds on the EU Cyber Security Strategy of 2013 and aims to further improve cyber resilience and response within the EU.

The components of the Package are as follows: a reform of the European Union Agency for Network and Information Security (ENISA), the creation of an EU certification framework and initiatives to promote security by design, and a presentation of ideas on how to further enhance EU-wide cooperation in case of a large-scale cross-border cyber incident or crisis.

Further considerations on updating the European Cyber Security Strategy must be made together with the Member States.

ROLES AND RESPONSIBILITIES IN EU CYBERSECURITY

What are the roles and responsibilities in EU cybersecurity? Let me highlight just a few points that might be relevant for the ensuing discussion:

Cybersecurity capacities and competences lie mainly with the Member States. A consistent EU cybersecurity policy must continue to support Member States in building their cybersecurity capacities; and create a suitable framework for joint action to protect common values in cyberspace as well.

The European Union Agency for Network and Information Security (ENISA) plays a key role in shaping the EU's cybersecurity policy. It is therefore right and necessary to give ENISA a stronger and permanent mandate. This will enable ENISA better to perform its important task of supporting the institutions of the EU and the Member States in ensuring cybersecurity in their respective fields.

Building operational capacities, however, has to be seen as a critical task. The prevention of cyber incidents and attacks by strengthening resilience continues to be the method of choice to adequately counter the risks and threats a digital society faces.

It is therefore essential that the Member States consistently implement the NIS Directive and get it off the ground in cooperation with the Commission and relevant stakeholders.

Building and expanding the Member States' cybersecurity capacities as provided for in the Directive is an integral part of a safe European Union. The EU, the Member States and the businesses concerned will be required to make considerable efforts in the months and even years to come.

Operational cooperation between the Member States, which is to be intensified through the CSIRT network, is one example. The sharing of information between the individual CSIRTs is based mainly on mutual trust. Sufficiently qualified and independent staff and suitable technical equipment are absolutely indispensable in this respect.

In order to handle large-scale incidents with severe national and cross-border impacts, cooperation among the Member States must be improved and intensified. With the CSIRT network, a central body for sharing information at the technical/operational level was set up. Once it is fully operational, the CSIRT network can make an essential contribution to ensuring common situational awareness by increasing the amount of information available at Member-State level to assess a specific situation. However, possible reports or evaluations within the CSIRT network can neither replace nor reflect the national position of a Member State. A common situational awareness can only be reached on the basis of national conclusions and evaluations.

Regarding cooperation with the private sector: it is important to place a focus on flexible instruments and call upon all those responsible for cybersecurity, namely the Member States and businesses. Promoting and expanding public private partnerships at Member-State and European level certainly might be one appropriate approach here.

A European initiative to drive Europe towards IT-security, aside from national solutions, is highly welcomed: We need reliable and transparent common IT security standards for the increasing number of connected products to build higher standards of resilience into products. Other third-party nations should be able to recognise these.

Also, European ICT Cybersecurity Certification is not only a matter of the Digital Single Market but is also of interest to the public and to the national security of the Member States. It must therefore be ensured that a future European ICT Cybersecurity Certification take the security interests of the Member States sufficiently into account. Furthermore, it is very important that the European achievements in ICT Security Certification will be saved and migrated appropriately from an activity driven by some Member States to a European institution.

The digital transformation represents a great chance, and cybersecurity is the major challenge of the future. The EU and its Member States are well prepared when it comes to ensuring cybersecurity. Now it is important to continue along this path and face the challenges posed by the digital revolution together with all responsible stakeholders.

Discussion: Procedural, Institutional, Technical and Management Devices

MARIE-CHRISTINE DÄHN

The final discussion of the conference focused on the 'on the ground' aspects of privacy and cyber security. The initial input was provided by Ira Rubinstein, Klaus Lenssen, and Rotraud Gitter, who shed light on procedural, institutional, technical, and management devices applied in the field. This more practical perspective complemented the previous presentations, which concentrated more on 'on the books' issues. Consequently, the discussion focused more deeply on practical issues as well, such as the implications for the internet of things (IoT) or product development.

As a general concern in the area of cyber security, it has been remarked that flexible ways of enhancing the security of technology would be of key importance. This could include incentives for companies, stricter liability for producers or more transparency for the users. The debate identified 'security by design' as a central issue in this direction, both in terms of the necessity of a proper legal mandate and the dissemination of best practices. One of the core problems the participants outlined is that users still too often have to decide between economical and secure technologies. Therefore, an essential future task, especially for producers, will be to bring affordability and security together so that there is no necessity to choose between them. Despite the different opinions on how best to achieve this, the participants agreed that, in the end, an open debate between all involved parties serves to lay the foundations for beneficial developments.

Nevertheless, there have been diverging views on where to start in making cyber activities more secure. On the one hand, the difference in the levels of requirement for cyber security in different countries, particularly in Europe, would lead to confusion and run against the internal market principle. Therefore, legal harmonisation has been considered necessary as it could provide more clarity and an equal level of security. The question remained, however, as to what degree of harmonisation would be most effective as well as acceptable for all the stakeholders involved. On the other hand, while the view has been shared that a variety of different regulations could impose problems, for instance, from a practical perspective it would be much wiser not to always typecast products in distinct and sharp categories based on different regulations. Additionally, it was pointed out that attention should also be shifted to technical practice more generally. In doing so, an analysis could be made of how products play out in their everyday use and whether they operate as expected. This would shift more focus onto the operator. Network behaviour anomaly detection could be an approach to implementing this. In

applying this method, the traffic of a network would be constantly monitored in order to detect anomalies or unusual events. There are, however, possible negative side effects associated with this approach. This constant monitoring of users' behaviour to compare normal network behaviour with that under scrutiny is severely criticised by privacy and freedom of speech advocates alike as it could also be used for surveillance or censorship purposes.

Another important strand of the discussion addressed the question of whether governments might need vulnerabilities in order to extract intelligence. It has been agreed that governments' intelligence activities do in part depend on such vulnerabilities, but this has to be balanced with the citizens' interests as most of them would strongly benefit from fixing (globally scaled) vulnerabilities.

Finally, the debate touched upon one of the main challenges of cyber security today: Which standards should and could be developed for the IoT? Since in an IoT environment numerous technical objects are connected and extensive amounts of data are generated, transmitted and processed, both privacy and cyber security issues arise. From a privacy perspective, one of the main problems is that the IoT not only connects information from public devices and networks, but also from private sources. Thus, a lot of personal data is gathered and potentially processed. From the cyber security point of view, there are many possible threats to consider in this regard: insecure web, cloud, and mobile interfaces or network devices, the lack of transport encryption, or insecure software, to name but a few. There are currently no sufficient responses to any of these problems —neither by single states nor from a transatlantic perspective. Certainly lessons can be drawn from other areas of cyber security and practices there, but the IoT environment has specific characteristics and imposes new challenges which call for further debate.

LIST OF PARTICIPANTS

Tyson Barker: Program Director and Fellow at the Aspen Institute in Germany
Wilfried Bernhardt: Lawyer; Honorary Professor of Internet Law, E-Government and E-Justice at Leipzig University
Théodore Christakis: Professor of International Law at the University of Grenoble; Dep. Director of the Grenoble Alpes Data Institute; Director of the Centre for International Security & European Studies at the Institut Universitaire de France
Marie-Christine Dähn: Student Assistant at the 'Global Privacy Governance' project at the HIIG
Christian Djeffal: Researcher and Project Manager 'IoT & eGovernment' at the HIIG
Karsten Geier: Head of Coordination of Cyber-Policies at the German Foreign Office in Berlin
Judith H. Germano: Adjunct Professor of Law at New York University; Senior Fellow at the NYU Center for Cybersecurity
Rotraud Gitter: Regierungsdirektorin at the IT and Cybersecurity Section of the German Federal Ministry of the Interior in Berlin
Zachary K. Goldman: Adjunct Professor of Law at New York University and Executive Director at the Center of Law & Security
Maximilian von Grafenstein: Head of Research Programme on 'Governance of Data-Driven Innovation' at the HIIG
Claire Groden: Program Associate at the Center on Law and Security at NYU School of Law
Sven Herpig: Project Director of the Transatlantic Cyber Forum at the Stiftung Neue Verantwortung
Julian Hölzel: Researcher at the Department of Computer Science at Humboldt-Universität zu Berlin; Associate Researcher at the HIIG
Gail Kent: Global Public Policy Manager at Facebook
Philipp S. Krüger: Advisor for Cyber Security at Fraunhofer SIT in Berlin
Christopher Kuner: Professor of Law and Co-Chair of the Brussels Privacy Hub at Vrije Universiteit Brussel
Mark Lange: Director of EU Institutional Relations at Microsoft
Klaus Lenssen: Chief Security Officer at Cisco Germany; Head of Security and Trust Office, Germany
Kai von Lewinski: Professor of Public Law, Media Law and Information Law at the University of Passau
Christian Marks: Student Assistant at the 'IoT & eGovernment' project at the HIIG
Randy Milch: Co-Chair of the NYU Center for Cybersecurity; Distinguished Fellow at the Center on Law and Security; Professor of Practice at NYU School of Law

Paul Nemitz: Principal Adviser to the Director-General for Justice and Consumers at the EU Commission
Luis Oala: Student Assistant at the 'IoT & eGovernment' project at the HIIG
Anke Obendiek: Research Associate and PhD Candidate at the Hertie School of Governance
Ingolf Pernice: fmr. Professor of Public Law, Public International Law and European Law at Humboldt-Universität zu Berlin; Research Director, Global Constitutionalism at the HIIG
Enrico Peuker: Senior Researcher, Law Faculty, Humboldt-Universität zu Berlin
Jörg Pohle: Co-Head of Research Programme 'Data, Actors, Infrastructures' and Project Manager 'Global Privacy Governance' at the HIIG
Reinhard Priebe: fmr. Director Internal Security in DG Home Affairs at the EU Commission
Frederick Richter: Director at the Stiftung Datenschutz
Ira Rubinstein: Senior Fellow at the Information Law Institute at NYU School of Law
Claus Schaale: Manager, Cloud Computing Business Development at Cisco Systems
Tim Stuchtey: Executive Director of the Brandenburg Institute for Society and Security (BIGS)
Michael Waidner: Professor for Security in Information Technology at the Technical University Darmstadt; Director of the Fraunhofer SIT in Karlsruhe
Lennart Wetzel: Manager Government Affairs, Corporate, External and Legal Affairs at Microsoft Germany
Thorsten Wetzling: Researcher and Director of the Privacy Project at the Stiftung Neue Verantwortung

IMPRINT

PUBLICATION
August 2018

EDITORS
Prof. Dr. Dr. h.c. Ingolf Pernice (HIIG)
Dr. Jörg Pohle (HIIG)

Alexander von Humboldt Institute for Internet and Society
Französische Straße 9
10117 Berlin
Germany
www.hiig.de/en

LAYOUT
Katja Margulis (www.lastica.berta.me)
Larissa Wunderlich (HIIG)

Softcover ISBN: 978-3-9820242-0-2
eBook ISBN: 978-3-9820242-1-9