DAY 1: SIGINT intelligence transnational activities: an introduction on knowledge and secrecy, law and technology dilemmas

Introduction:
Alain Dieckhoff, director of the CERI gave the welcoming speech in which he emphasised the diversity of the participants of the event and expressed his high expectations regarding the products of the UTIC group.

Didier Bigo then introduced the three-day colloquium by presenting the research question: *how to conduct research on secret services?* How to gather knowledge on professionals that are legally compelled to keep secrets? He sketches *the main paths of access to information* beyond official documents, in this well-guarded area:
- Interviews with former actors, whose discourses reveal that the administrative practices in secret services are not fundamentally different to those that can be found in other administrative or corporate services with similar purposes.
- an increasing number of academic centres on training of future members of secret services allows learning about their main concerns and directions by reading the programme studies
- reports from oversight bodies, who are nonetheless legally constrained, despite a significant evolution of their role after 2013 and more details on scrutiny
- documents released by whistle-blowers, who by definition are not bound by the same restrictions as other actors, and a reflexive stance on their conditions of production
- discussions with investigative journalists, whose mission consists in breaking secrets, by distinct means
- academic research

Bigo stressed that it is not a matter of choosing one source or the other, but to combine and confront them. *Since a secret is, by definition, shared, it is crucial to study its logic of circulation,* even more so now as the information flows have grown exponentially. Who shares secrets, and with whom? Who does not share? He stresses how important it is to take into account the historical evolution and to avoid a “black box” imagery.

Subsequently, Laurent Bonelli reflected on how to render research on secrets less intimidating. The fact that the secret is very widespread, in a variety of social universes, draws it away from magic. On the contrary, as shown by Simmel, the secret is a “sociological pattern” which delimitates groups, rests on trust and increases the perceived importance of who pretends to hold it. There is *no superiority of secret information,* in other words it is not, by itself, more relevant or more truthful than public information. What distinguishes both are the social conditions of production, circulation and communication. Information is a product of the social world, it *must be objectivised and treated with the regular tools of social sciences,* in combination with other disciplines such as engineering and law, even more so in a context of fast technological and legal changes. He finally exposed the three principles of this kind of research: a comparative stance (that highlights similarities between agencies operating in different countries), historicity (with a focus on routines and transmission) and attention paid to practices (which allows going beyond justifying discourses from the actors).

Finally, Sébastien-Yves Laurent took stock of the three years of the UTIC research. The group explored eight axes of research, in three broad directions: the *technical dimension* of surveillance, the
practices of intelligence (including interstate and public-private cooperation), and the laws regulating them (at the national, European and international levels).

Panel — “SIGINT intelligence - law and technology: knowing and understanding of security technologies, secrecy and national security”

Philippe Guillot introduced the deliverable he produced with Daniel Ventre about the use of interception technologies, with a focus on its historical, technological and legal dimensions, as well as the presentation of the actors involved in interception and what is at stake in cryptology. They have observed a large amount of similarity between the missions of interception services through time, even over centuries. Interception comes hand in hand with communication and evolves in parallel. They distinguish different kinds of interception: at the source or in transit. The tools used for interception are software placed on the routers or the targets. While cryptology was considered as a war weapon since WWII, several Western European countries adopted laws at the turn of the new century to allow its use. The transition from one regime to the other was not without tensions, as revealed by, for instance, the “Clipper chip” or the “trusted third party” episodes at the beginning of the 90s. However, encryption can be bypassed, for instance by finding vulnerabilities in public keys or protocol failures, as well as by imposing backdoors (as Australia and the UK, among others, are currently trying to do).

Second panellist Maxime Kelhoufi addressed the issue of the secret of correspondence and data protection in relation to the 2015 French Intelligence Law (Loi Renseignement). How does this law stand in front of the EU law? While the Intelligence Law forces the telecommunication operators to intercept and store certain metadata - and to hand them in to the services when requested - this obligation contradicts a 2002 EU directive on the processing of personal data and the protection of privacy in the electronic communications sector. The French state Council (Conseil d'État) has recently introduced a series of prejudicial questions before the Court of Justice of the European Union, whose answer is expected in the following months. While there are reasons to expect a ruling against this prior and generalised collection of personal data for violation of articles 7, 8 and 11 of the Charter of Fundamental Rights, this outcome cannot be taken for granted since the Court may also consider that these human rights-related concerns are appropriately taken into account by the introduction of safeguards such as the role played by the CNCTR (National Commission of Control of Interception Techniques), or the fact that “only” metadata (not the contents of the communications themselves) are collected. Should the Court validate the Intelligence Law, it would mean a significant evolution of its jurisprudence based on the 2016 Tele 2 ruling.

Third panellist Bill Robinson described the main features of the Communications Security Establishment, the Canadian signals intelligence agency, created in 1946 and now with 2,300 employees. According to a law passed in 2001, all interceptions of domestic communications (communications with at least one end in Canada) must be previously approved by a judicial warrant (for law enforcement agencies and the domestic security service, which is responsible for, e.g. counterterrorism activities) or a ministerial authorisation (for signals intelligence). Interceptions of international communications (those with both ends outside Canada) are not submitted to such requirements, even if there is a Canadian person on one end (as long as it is not the targeted one). Concerning the collection of metadata, no warrant requirement applies so far but a law currently under discussion in the Parliament will require CSE to obtain a “quasi-judicial” authorisation by a semi-independent commissioner. It is seen as having high chances to be adopted soon. A high volume of information is shared within the Five-Eyes group and, to a lower extent, also outside this group, in particular with European agencies. The sharing takes the form of, for instance, selectors that are applied to the interception systems of the different participating countries. Once these selectors are approved, the information collected is provided without any kind of further approval being necessary. Metadata are also widely shared, although with strict minimisation requirements when they are about
Canadian nationals. Processed intelligence, in the form of reports, is the most routinely shared intelligence: around 10,000 SIGINT reports a year from Canada, once again with strict data minimisation or removals when referring to Canadians. It is important to recognise, however, that intelligence sharing among the Five-Eyes goes well beyond the sharing of signals intelligence. Robinson also stresses the fact that the Canadian service receives more information than it could possibly process with its current workforce. A review commissioner, created in 1996, publishes a yearly report, but is subject to strict conditions regarding the information that can be revealed in that document. However, the above-mentioned law currently under discussion is expected to create a new review agency with a broadened role. Finally, in 2017, a committee of parliamentarians was established to look into the functioning of the Canadian intelligence system on a continuing basis: how well this committee will function remains to be seen, but its creation has raised hopes.

Fourth panellist Claudia Aradau presented how intelligence practices have been transformed by digital technology, to the point that they can now be considered as “big data organisations”. Her focus is on programmes, such as Skynet, that produce the figure of the suspect through the detection of “anomalies” (or irregularities) in big data. It concerns telephone communications or travel patterns. As confirmed by some of the documents revealed by Snowden, anomaly production has become a key practice through which intelligence services now deal with the “unknown unknowns”, where there is no previous knowledge at all about the target and the query. She insists that this proceeding is distinct from the establishment of a norm and the identification of deviations from it: it rather consists in identifying small groups isolated from topological density. In June 2018, a US Court dismissed a journalist’s claim that he had been wrongly included on a kill list on the basis of such algorithmic criteria. However, it admitted another similar claim by another journalist that was grounded on him being actually targeted five times. This raises the issue of the adequate standards to assess credibility, with competing answers from the legal, statistical and intelligence perspectives. The transnational scope of the effects of such practice brings further complexity. Combined, those elements make it even more challenging to find a proper way to apply oversight on intelligence activities.

In his comments on this panel, Bertrand Warusfel raised two points. First, that the digitalisation of the means of communication has brought a paradigmatic change which increased the autonomy of the SIGINT branch within intelligence services: it is now much more efficient to massively gather information, for further analysis through ever-progressing algorithms, in contrast with the past when information was mostly collected through human means, with only a complementary role given to the technically-driven collection of mass data. Additionally, the predominantly anti-terrorist aim of current intelligence action requires not only to identify suspects but also to detect their intentions, in order to be able to prevent them from causing harm before it is committed. This purpose constitutes another rationale for using those computer programmes, that are expected to have predictive capacities. A “race to data” follows, since the intelligence services (as well as other actors in the private sector, for their own reasons) want to be able to “train” and to improve their algorithms, along a “machine learning” logic. He refers to Antoinette Rouvroy, a Belgian writer who highlighted “algorithms governmentality”, meaning that, if they are not specifically tested against this risk, the algorithms introduce biases and distort the reality they are supposed to depict. Second, those transformations require a strengthening and an adaptation of the oversight mechanisms. To be effective, control agencies need to have means and resources to perform their activities, a requirement that is increasingly hard to meet in a context where, in Calvar’s words (from DGSI) “technology is evolving so fast that only machines will be able to control machines”. To conclude, Warusfel suggests that a means to adapt to such a challenging time could consist in pooling resources and know-how among the different control agencies that, beyond surveillance, face the same techniques and pursue complementary objectives.

In the Q&A, questions were raised about the role the French CNIL could play to control the way algorithms are used (it would be very limited in this area) and whether the automated decision-
making process falls under article 22 of the GDPR (it does, but in practice this right could be claimed only a posteriori). Elspeth Guild also highlighted that a common concern among several presentations was the tendency towards the “othering” of citizens. Laurent Bonelli makes a call to avoid conceiving those practices as uniform under a common logic, whereas they are, in fact, highly differentiated across services, time and places. Didier Bigo questions the alleged improvement of artificial intelligence through time, and even its designation as “intelligent”, referring to Meredith Broussard’s recent book Artificial Unintelligence: how computers misunderstand the world.

ROUND TABLE — “HOW WE CAN BUILD KNOWLEDGE ON INTELLIGENCE ACTIVITIES”

After an introductory statement by Philippe Hayez presenting the role of education and knowledge in matters of intelligence and the necessity to have a better understanding of the professions of intelligence, their necessity, their training, Alexandre Rios-Bordes stated that he used a “historical ethnography”, aka “retrospective ethnography”, as a key method to understand how intelligence agencies build their own knowledge. He qualifies this approach as a “break-in [effraction] through the past”. He studied two military services: the Office of Naval Intelligence and the Military Intelligence Division. Both were created in the 1880s to conduct external surveillance but were assigned an internal role after WWI. As an outsider to those services, Alexandre Rios-Bordes decided to rely exclusively on archives. He rejected the conception of such internal surveillance as a “pathology” and tried to understand the worldview developed from within by such services. He noted that the concepts of “modern war”, “inside threats” and “national security” were instrumental to internally justify their actions and to provide a ground for their reason to be. The examination of daily administrative correspondence was key in his research, in particular to indirectly detect instances of the two main techniques used to hide the existence of sensitive activities: orders given orally and the physical destruction of evidence. This source of information allowed him to avoid an anachronistic interpretation of past practices: he was able to “watch them” work, produce knowledge and develop their routines in the context of what he calls a “bureaucratic banality”. Among them, he highlights the construction of different categories of threats and the drawing of the “figure of the adversary”, which by then was not associated with terrorism but subversion. Rios-Bordes finally describes the four tensions that he found across intelligence services: the use of techniques to build up a strong internal legitimacy as a compensatory action in front of their low external legitimacy, the contrast between their aspiration to know everything and the practical impediments to that goal, the challenge of credibility, when channelling relevant information through higher levels of authority and the seemingly incoherent articulation between the internal and external threats.

Second panellist Sharon Weill shared her experience as a researcher specialized in terrorism trials, which includes hard-to-access courtrooms: The Israeli military courts, the Guantanamo Military Commission and the French “Cour d’Assises” specially composed for terrorism cases in Paris. She stressed a paradox: on the one hand, a trial is expected to be transparent and accessible to the public but on the other hand there is a need for the inclusion of the secret services in the proceedings to establish the facts, despite the fact that their activities are supposed to be hidden from the public. She stresses that her aim is not to get access to secret information but to observe how secrecy is managed and eventually revealed – or not - in a tribunal. This tension is resolved differently in criminal and administrative procedures. For example, in administrative courts in France (which have a closer linkage to the executive) the use of secret evidence in form the “white notes”, which are delivered by the services are deliberately vague (e.g. no date, no signature) can alone be the legal basis for far-reaching measures against the persons. This same information will not constitute admissible evidence in a criminal trial. This is the case also in proceedings in other courts such as in Israel: while certain evidence will not be admissible in a criminal trial they will be in an administrative one. Thus, the administrative procedure replaces the criminal ones when necessary. In contrast, at the French Cour d’Assises,
the information is extremely transparent. The principle of the ‘Orality of the debates’ imposes that only evidence and testimonies that were presented and debated orally at court are admissible. In terrorism case there is no jury and the bench consist of 5 judges. Yet only the President is allowed to read the file. All the other judges ‘discover’ the facts and evidence with the public- as a popular jury. A very interesting example was the Merah trial, where the heads of the central security service and of Toulouse came to the court and gave contradicting testimonies. In common law system this would be a very unusual situation. This trial brought brand new information to the journalists that were present there. However, as in France no transcript is published afterwards, physical presence in the courtroom is a necessary condition to get access to such information.

Access to the trial, to the file and the court decisions can be difficult to access both to the accused and the researcher; in Israel, the military courts are to be accessed through a military base. In France, access to court is public. Yet, it is very difficult for a researcher to obtain information on the calendar of the hearings. Although technically public, obtaining court’s decision is very complicated and depends on personal relations with the clerks or the different actors. In Guantanamo the criminal trials are almost impossible to access. Yet, all the transcripts of the military commissions proceedings are available online, although sometimes heavily redacted. In her final words about Guantanamo, she explains that in the Guantanamo proceedings, in the public gallery or in the filmed sequences that the journalists and NGO members have access to from another part of the military basis have a 40-seconds delay, so it can be cut at any time, by the judge or the secret services themselves, if necessary, to preserve sensitive information.

Third panellist Anne Charbord, who has been working on security and Human Rights issues for the past 12 years, showed how the right to privacy has become a central issue within several key UN Human Rights mechanisms. She underscored the pivotal role of the Snowden revelations in the adoption by the GA of the first resolution on the right to privacy in the digital age in December 2013 (68/167). It launched a series of steps that firmly established the right to privacy as a central human right. After a significant push from Brazil and Germany, the UN General Assembly adopted a Resolution on the Right to Privacy in the Digital Age in December 2013. Its adoption opposed on the one hand the Five-Eyes countries and on the other a large coalition led by Germany and Brazil. The main points of contention concerned the application of the principle of extraterritorial application of the right and the principle of distinction between national and foreigners, as well as on whether mass surveillance could constitute a human rights violation. The adopted compromise text, while weaker than the proposed text, nonetheless refers to the 'negative impact on the exercise and enjoyment of human rights' of 'extraterritorial surveillance'. It also affirms the principles that 'the right held by people offline must also be protected online' and establishes that surveillance is a human rights issue, to be examined within the human rights framework of the ICCPR. In 2014, at the request of the GA, the High Commissioner for Human Rights issued a report on “The Right to Privacy in the Digital Age”. The report further elaborated on the right to privacy and recalled that the right to privacy is a platform right, necessary for the exercise of other rights such as freedom of expression and political rights; that any capture of content or communications data can be seen as an interference with the right to privacy, whether the data is accessed or not; that any interference with the right to privacy must comply with the principles of legality, necessity and proportionality; in response to the question of extraterritorial application - stated that digital surveillance engages a State’s human rights obligations if it involved the State’s exercise of power and effective control in relation to digital communication infrastructure, wherever found; and that any difference of treatment between citizens and foreigners is a violation of the principle of non-discrimination. A number of procedures and mechanisms have since further elaborated on the right to privacy, including through the creation in 2015 of the position of in 2015 “Special Rapporteur on Privacy”, thus placing the right to privacy clearly on the agenda of the UN. Finally, Anne Charbord reflected on a possible “Magna Carta for the Internet”. With several projects on the table, the Special Rapporteur on the right to privacy has focused on the question of legally-binding
document. He presented a draft in 2018 on 'government-led surveillance and privacy' which aims to provide States with a set of principles and model provisions for integration into national law. While there is some agreement that the current state of implementation of the right to privacy online is piecemeal due to a lack of substantive, jurisdictional and procedural certainty, many States nonetheless uphold the position that there is no need for a new legal instrument as international law provides a clear and universal framework for the right to privacy. Civil society, for its part, highlights the risks of an approach which could lead certain governments to further encroach upon freedom of expression.

Fourth Panellist Guy Rapaille has been the head of the “R Committee” (the Belgian oversight body for intelligence activities) for 12 years. This organ can be compared to what an “Independent Administrative Authority” is in France, it reports in broad terms to the Parliament and in a more detailed fashion to the Minister of Defence. The speaker stressed the fact that the Belgian law only allows surveillance of organisations or institutions (not individuals) and that bulk surveillance is illegal. He also clarified that in Belgium SIGINT has a narrower meaning than in other countries, since it designates the interceptions of communications that are originated in, or destined to, foreign states. The R Committee is in charge of controlling this narrowly-delineated SIGINT, which is operated exclusively by military intelligence services in the name of the protection of Belgian troops and civilians located abroad. There are three kinds of controls. The first one is a priori: the intelligence services draw a list of organisations and institutions whose communications they want to intercept: this list must be motivated, and the R Committee can assess the validity and scope of such justifications. The second kind of control takes place at the same time as the interception itself: if the Committee can visit the place where the technical process is taking place and, if it considers that the given authorisation is not being respected, it can impose an immediate end to the process and the destruction of the material that has already been collected. The third type is a posteriori, after consulting the monthly logbook of the intelligence service. The panellist closes his remarks by highlighting that the R Committee is in the process of further developing the technical side of its controlling activity, in order to keep up with the challenge of the evolution of the interception methods.

Fifth panellist Aurélien Gloux-Saliou, general secretary of the Commission Nationale de Contrôle des Techniques de Renseignement (CNCTR) started by exposing the fact that this oversight body controls all technical means of gathering intelligence which infringe on someone’s privacy, from the most to the least intrusive, either on a domestic or an international scale. Therefore, its mandate is not limited to the techniques designated as “SIGINT”, which in fact is not recognised as a specific category in the French law. The CNCTR, with 17 employees and a 9-member board, is relatively recent: it was created at the end of 2015, in replacement of the CNCIS (Commission Nationale de Contrôle des Interceptions de Sécurité), which had a more limited range of action. The control applies to all intelligence agencies, whether they are services specifically entrusted with the collection of information (for instance the DGSE or the DGSI) or law-enforcement agencies which may occasionally resort to surveillance measures. Mr. Gloux-Saliou emphasised that this control has been working so far, as the CNCTR observes that the intelligence services are willing to respect the legal framework which limits their activities within the proper margins and ends up protecting their action. The a priori control consists in the CNCTR providing an opinion to the Prime Minister, before he authorises (or not) the implementation of a given intelligence gathering technique. While the 2015 Intelligence Law was imposing a CNCTR opinion only for domestic surveillance, an informal agreement between the oversight body and the Prime Minister made this opinion routine for both domestic and international communication interceptions. The recent Military Programming Law, adopted in July 2018, converted it into a legal requirement. In the statistical part of his presentation, he indicates that 70,000 opinions have been delivered last year, two thirds of which regarding access to connection data. For the first time, last year an authorisation was given to operate an algorithm, applied only to connection data and aiming at detecting terrorist threats.
Terrorism prevention represents half of the requests for surveillance. The \textit{a posteriori} control can take place in the venues of the intelligence services themselves: there were 60 of this kind in 2016 and more than twice this number in 2017. The CNCTR voluntarily discloses the number of individuals that are the object of at least one intelligence technique: 20,000 in 2016 and 21,000 one year later. Individuals have the right to ask the CNCTR to verify whether or not they have been unlawfully put under surveillance: in 2017, 60 people made such a request. If the CNCTR finds any irregularity in the proceeding of an intelligence agency, it can recommend the Prime Minister to demand the end of such a practice and the destruction of the information already collected. If its recommendation is ignored, it can bring the case before the Supreme Court for administrative justice (Council of State). Mr. Gloux-Saliou finishes his talk with the assertion that the oversight body is making sure that the French law about surveillance is being respected: so far, \textit{only minor irregularities have been detected} and they have been rectified at a later stage. However, he admits that the conformity of such law against European standards still needs to be verified by both the ECtHR and the CJEU, which are currently examining it.

Among other questions during the Q&A session, Didier Bigo asked whether the oversight bodies are able to control the collaboration between national intelligence services and to overcome the limitations of oversight regarding the third party rule and the national security of other states. Guy Rapaille indicates that this is currently not the case, despite a recent and embryonic initiative from the bodies of some small countries, which is facing harsh legal and practical hurdles. Theodore Christakis wonders whether there is an obligation to notify people who had been subject to surveillance: whereas notification is possible in Belgium, it is only for Belgians, on demand and after ten years. It is forbidden in France: the CNCTR cannot either confirm or deny that a surveillance technique has been applied. Another question from the public allowed to highlight the fact that, in addition to the 20,000 people being directly targeted each year, there are more individuals whose information is being collected, because of their communications with the targets themselves.

\textbf{DAY 2: Sharing secret information: Current transformations regarding the nature of the threats, the actors involved in intelligence activities, the necessity to use surveillance, its scale, intrusiveness, and its impact on privacy and social behavior of Internet users}

\textbf{Panel 1: “Global Alliance, National Sovereignty; Sharing Secret Information Dilemmas”}

This panel focused on the collaboration between SIGINT agencies around the world, with the aim to assess whether this collaboration is simply led by the Five Eyes with concentric circles around it, or whether there is a transnational guild based on the capacity of extraction of information from Internet sources.

In her research, the first panellist Ronja Kniep examines data sharing practices and its limits of the Five Eyes, and beyond. She described the \textit{Five Eyes} as a network embedded in a transnational field, compartmentalised and differentiated with asymmetrical power relations and unequal access to data. The second-party partners comprise the UKUSA community, i.e. the Five Eyes themselves (UK, USA, Canada, New Zealand, Australia), and third-party partners such as NATO members, Nordic countries (such as Sweden) and Taiwan and Israel, and thus extend beyond Western communities. Within this bigger framework, the \textit{NSA constitutes the central node which spies also on third parties} and has its own agreements with domestic agencies. Sharing practices are conducted under a high level of secrecy, with mutual benefits, with the understanding that foreigners are “fair game” while own citizens are legally protected. \textit{Under this framework, bilateral sharing is more
comprehensive than multilateral sharing. Other multilateral agreements include the SSEUR (SIGINT Seniors Europe) and SSPAC (SIGINT Seniors Pacific), hosting annual workshops and conferences. However, there remains a gap between them and the Five Eyes. In conclusion, there are increasing data sharing practices within the transnational field of SIGINT. Moreover, it is important to resist the temptation to overemphasise unity of sharing practices and between actors. Reasons for not sharing data include competition for limited resources, security concerns, and institutional and cultural differences between agencies.

Second panellist Thorsten Wetzling examined the case of the German BND and its “double allegiance”. He argues that Germany’s exceptionalism has to do with the governance and coding of SIGINT in Germany. The first allegiance is that of the BND to itself as the core of national sovereignty. The second allegiance is based on bilateral cooperation with the US at the core and instantaneous data sharing, and multilateral allegiance with the SSEUR. In the 1980s/90s the BND had to catch up with other intelligence services with regards to technological developments. In order to deepen relations with the US and in exchange for software, it underscored the central importance of Frankfurt as an Internet hub with optic fibre cables, as well as its embassy premises in other countries which offered vast access to foreign data. In 2016, Germany changed its intelligence legislation and enhanced the protection of European data in terms of the SIGINT protection. Any new cooperation between the BND and a partner requires an agreement on the aim and the nature of it, respecting the fundamental rule of law and usage for the intended purposes. Considering the array of intelligence partners, are these conditions merely cosmetic? This certainly raises a need for oversight cooperation.

The third panellist Steven Loleski focused on the resilience and expansion of the Five Eyes community into cyberspace by exploring its dynamics as a community of practice. During the Cold War when there was a greater incentive to formalise the NSA’s alliances with its junior partners into a multilateral pact to optimise foreign satellite collection, these relationships largely remained bilateral. Yet, at the height of American unipolarity and capabilities, the relationship was formalised into a multilateral pact in 1993, a senior steering group to manage its relations in 1998, and beginning in 2003, a series of annual conferences and workshops to support joint activities. As the NSA transformed to deal with the challenges confronted by cyberspace, it was not a forgone conclusion that cooperation with its allies should extend to signals development activities designed to support computer network operations. In order to understand why the Five Eyes had evolved into a multilateral pact largely coordinating its foray into cyberspace, we need to focus on the partners constituting a community of practice. In other words, it is people, processes, and policies pushing collaboration across a number of peer-to-peer relationships that create the opportunities for spillover.

Fourth panellist Didier Bigo presented a deliverable that he developed as part of the UTIC ANR about the data politics of suspicion in intelligence matters and the collaboration of intelligence services between democratic regimes. He began by deconstructing the notion of ‘national security’, which is often used without sufficient attention to its meanings and even more importantly its practices. The meaning of ‘national security’ as a key element of sovereignty becomes destabilised when ‘national’ data has been constructed through shared interception of information and also shared results with foreign partners. It is important to denaturalise the image that intelligence communities work ‘nicely’ together as different national epistemic communities of a global alliance sharing key values, and instead to point to the structural elements of each agency in terms of their use of techniques and their habitus in producing lists of suspects in Europe. Solidarity between the latter is higher than between the former, but this was almost invisible. ‘National security’ has been for years a form of consensual narrative masking the heterogeneity of practices between police and military institutions and the variety of their goals, creating the image that intelligence officers obey their national political masters spontaneously. However, different cases such as the extraordinary rendition complicity around
The CIA, the Snowden revelations on the large scale surveillance organised by the NSA and its network of allies, the politics of drones by the militaries, the role of the DIA, the NATO networks and so on, including the case of the BND informing the NSA against its politicians, show the relative disconnection between the national politicians and their different national services, and the strong connections that may exist between services using the same kind of techniques transnationally, a relation that can be called the emergence of transnational guilds into the field of the techniques of extraction of information intelligence. The Snowden disclosures have showed the extent of such a large-scale surveillance on Internet users done by the guild of the Five Eyes Plus network in the name of prevention of terrorism, but mainly done for other purposes reinforcing their resources and symbolic power. In reaction to the Snowden disclosures, the secret services have immediately produced a counter-narrative that this extent of surveillance was only an illusion, that they were targeting specific individuals and that in fact, personal data were not shared this broadly, but filtered. In light of this controversy on the scale and effectiveness of intrusive surveillance, it is important to analyse what exactly the practices in the name of national security are and who precisely defines what the national interest of the state is and how this sovereign interest is constructed and justify derogation to common democratic rules. In the case of large-scale surveillance, how far do intrusion and data mining go? What is the validity of the interception of personalised and anonymised data helping to construct profiles of suspicion? Are they effective or do they further perpetuate the narrative of ‘preventing’ scientifically by knowing the behaviour of individuals before they can act themselves via algorithmic analytics and machine learning? Bigo argues that this notion of scientific prediction has been rejected by computer scientists, while public discourse continues to perpetuate it, often for commercial purposes. In light of this, we have to reconsider the relationship between the intelligence officer and the politician; the intelligence officer does not merely obey the politician; instead the politician is driven by a logic of data suspicion.

The panel concluded with comments by Andrew Neal. He drew attention to the stakes and the conditions of possibility for these kinds of interactions and practices. What kind of political class have we, and what is the role of parliament and back-benchers? Do they abandon their role on intelligence purposes or do they involve time into it to become specialists? How is representative democracy working in different national context? Some of the central themes in these interventions concern the knowledge on the technological nature of interaction, such as the process of construction of databases, and the power of algorithms and selectors based on profiling as the main tool of information sharing beyond identification. Moreover, to what extent are these interactions depoliticised, what is the role of public debate and democratic oversight? Another central question raised from the audience during Q&A was the purpose of mass surveillance which is often not clearly defined, either by the actors or even the analysts: Why is it done?

Panel 2: “Public-private assemblages and resistance to surveillance”

First panellist Félix Tréguer’s presentation consisted in presenting a deliverable that he developed as part of the UTIC ANR: “(Re)configuration of Public-Private Assemblages in Internet Surveillance”, with case studies focused on the USA and France. He stressed that public-private alliances to control communications is not new, but it dates back to the origin of the printing press. Now, this “assemblage”-style cooperation goes beyond media companies to also embrace the digital companies, which were supposed to adhere to a more liberal ethos. The PRISM program, revealed by Snowden, is a particular form of such cooperation, and one that is revealing of the clash between digital rights and certain actions taken in the name of security. Félix Tréguer indicates that, in the context of this “power struggle”, the resistance shown by the companies in front of government surveillance is partly “staged”; the transparency reports, published for instance by Google, give some notion of the real scope and upward tendency of such cooperation. In the encryption issue, recent instances of accommodations can also be found. The legislative innovations, be they already in force (CLOUD Act in the USA) or under discussions (e-evidence regulation in the EU) indicate that this trend is going to go on. Similarly,
the continuing efforts from the public authorities to have the companies regulating contents online, in the name of the fight against terrorism, belongs to the same logic. Such an indirect way to enact governmental objectives bears similarities with the process, described by Foucault, through which the modern judicial system progressively developed since the 14th century. This privatisation of law enforcement, which is consistent with Hurt and Lipschutz’s view of a “hybrid rule”, comes together with forms of automation by using big data analytics. Félix Tréguer concluded by stressing that such tools transform the bureaucratic practices in the different actors involved, in security issues and beyond, and raise serious question in terms of rule of law.

Bertrand de la Chapelle, executive director of the Internet and Jurisdiction Policy Network, expressed comments throughout the panel as its moderator. He stressed that the concept of profiling, born in the police area, has now moved to the marketing and advertising sectors, where businesses routinely rely on it. The companies are natural targets for law enforcement and surveillance activities since they do not only have data but also the capacity to process it.

Second panellist Matthias Schulze talked about “Governing 0-day exploits on a global scale” from a game theory perspective, following the model of the prisoner’s dilemma. He showed that each individual state has a proper interest to stockpile knowledge on 0-day vulnerabilities (which leads to a “digital arms race”) and a collective interest in having all such vulnerabilities reported so they can be patched to ensure the security of the network and computer systems. As game theory teaches us, the rational calculations create a suboptimal situation, a Nash equilibrium where free-riding is preferred to cooperation. Therefore, there is a need to create incentives to modify the way the actors identify their best interests. Among the incentives that can be theoretically envisaged, Matthias Schulze suggests decreasing the cost of cooperation (through programmes of vulnerability disclosure and /or bug bounties) or increasing the cost of non-cooperation (through sanctions). He compares Internet safety to a “global commons” and identify other regimes that apply in more traditionally-defined “global commons”, such as arms control, fishing quotas or the management of the Antarctic area. This comparison allows him to broaden the scope of possible solutions to this original “tragedy of the commons”. If zero-day vulnerabilities are conceived as an exhaust of the digital world, maybe a system to deal with them could be designed following a logic similar to the CO2 emissions marketplace, where programming mistakes would be allowed only in limited amounts and be assigned a cost.

Bertrand de la Chapelle took this issue as an additional confirmation that the framing of a problem is the first step to address it and key to determine how it can be solved.

This remark fully applies to the presentation by third panellist Lina Dencik about “Surveillance realism, resistance and the limits of techno-solutionism”. She presented the result of a research on “Digital Citizenship and Surveillance Society”, which had been conducted between 2014 and 2016, with ten focus groups and eleven interviews, with the purpose to understand how the Snowden leaks have transformed the relationship between the UK state and the citizens. She made clear that such revelations had a deep effect, since they brought down the idea of digital citizenship as a means for empowerment and normalised surveillance in our everyday lives, giving way to what David Lyon calls a “surveillance culture”. Among the findings of her research was the fact that people do worry about surveillance but feel powerless in front of it. This resignation, that she calls “surveillance realism” can be linked with the incapacity to imagine alternatives, in spite of the visibility of injustices, in a way that is similar to the “capitalist realism” described by Mark Fisher about the reactions to the 2008 economic crisis. She stresses that such a view was echoed in media coverage and policy debates. The main answers that are developed are shaped by such an understanding: anonymisation and encryption technologies revealed an atomised (i.e. individualised) strategy, as if no solution could be designed at a structural level. Advocacy groups outside the digital field did not feel engaged with the wide-ranging consequences of digital surveillance. These attitudes together converge into
framing the issue as an individual problem that can be addressed through technological solutions. As a consequence, the dominant framing is expressed in terms of efficiency and security to be reached, at the expense of individual privacy and data protection. Thereby the broader picture and the political dimension of the picture is missed: the spreading of a form of governance organised around the notion that behaviours can be predicted and pre-empted when necessary, thanks to the information extracted from our “data doubles”, all of this in the context of a deep information asymmetry. This also has to be compounded with considerations about the role of private corporations on our lives, social justice and democratic accountability. Resistance must engage other types of stakeholders, and both users and practitioners.

Bertrand de la Chapelle raised the idea that a form of “techno determinism” (as exposed in the book “What technology wants”) is also developing in front of “techno solutionism”.

Fourth panellist Grace Eden introduced her research on “Technical Standards and the Making of Surveillance Infrastructures”, which relied on interviews with people working in the standard-making process. She emphasised that the standards that she defines as “agreed characteristics that facilitate compatibility across products and processes within a particular domain” are agreed through a social process, which takes place transnationally involving different working groups, in a setting where influence capabilities are unequally distributed, in particular because of variations in market power. Despite their seemingly technical nature, stakes are high in standards since they “intersect with governance processes and the concerns of sovereign states since they shape the conditions under which digital citizenship is exercised, including how free speech, censorship and surveillance are enacted”. This is why she considers that a market-led approach is not the best model to make decisions on such a topic. The implementation of some standards can become overly difficult because of the compromises that are necessary and which can affect their operability and generate vulnerabilities. As revealed in the Snowden leaks, the NSA made sure it was involved in the standard-setting process. Grace Eden then showed how a high level of interoperability has allowed the development of initiatives that tend to generalise the surveillance logic. She cited the very diverse surveillance (and still operating) programmes in the USA, the all-encompassing Social Credit System in China (whose “gamification” logic is exposed), the wide-ranging Aadhaar register in India and the EU programme that promotes the Internet of Things, which, at the end of the end, consists in connecting everything together and may end up rendering the GDPR ineffective. Although the European courts are expressing concerns regarding the use of that much data in interconnected systems, those concerns do not appear to be shared in other parts of the world. Finally, the direct contribution of private companies in the massive collection of data may well be a way to legitimise the surveillance infrastructure that is being put into place.

Bertrand de la Chapelle highlighted the fact that the day-to-day surveillance embraces much more than the activity of the spying agencies. He also contrasted the “inchoate” nature of governance on the Internet (policy issues regarding its uses) with the advanced ecosystem of institutions that characterises governance of the Internet (protocol development and infrastructure issues).

In his comments, Daniel Trottier underscored the “multi, or at least bilateral” functioning of the surveillance system, with the government patronizing the big platforms to cooperate to its own purposes, which has unintended consequences or afterlives especially in relation to access to data. When it comes to content regulation, the platforms in turn deputise their users to flag illegal or inappropriate content. This practice can be “weaponised” against opponents or disproportionately affect women or minorities. He also expresses worries that some individuals, including celebrities, close their social accounts in order to avoid suffering from abuse online or different forms of surveillance. He points to the fact that a surveillance logic is at play in several professional sectors, through the rating system.
Theodore Christakis’ comments covered several aspects. First, he contended that the “outsourcing” of content regulation to the private sector in very diverse fields will put a heavy burden on small actors and widen the censorship capacity of the state, since the focus is not only on illegal, but more broadly on “risky” contents. Regarding the cross-border access to data, he asked a more “provocative” question: what if the corporations were, in this specific area, better than the states at respecting the users’ human rights, thanks to the economic incentives that underlie this process? Regarding the 0-day exploits, he argued that banning their use by the states would push them into using even more intrusive techniques to get access to data. Finally, he considers the “right to be forgotten” as a useful item within the “digital self-defence” toolbox. Encryption has its place there too, but the EU has a very contradictory approach on this issue.

After the Q&A session, Bertrand de la Chapelle closed this session by reminding us that the three objectives of fighting against abuse while respecting human rights and preserving the opportunities provided by the digital economy form a system and should not be treated as silos. They are tightly interconnected issues, so any attempt to solve a problem along one dimension will have an impact on the other areas.

Panel 3 “Authority and legitimacy of intelligence: the services’ operating logic in the surveillance of foreigners and citizens”

François Thuillier introduced the speakers and highlights the fact that the next presentations will cover a variety of Western states.

After a criticism towards what he calls “an analysis without actors”, which bring together all “intelligence services” as if it was a single, homogeneous bloc, Laurent Bonelli proposed a classification of such services, based on an objective and thorough analysis of their main missions and properties. Nine variables and 25 services from a dozens of different states are included in the research. A “multiple correspondence analysis” allows to identify three main poles: the “highly technoligised” (where GCHQ and NSA belong, among others), the exterior-oriented (MI6, CIA, DGSE…) and the interior-centred services (FBI, MI5, DGSI…). He observed that there is more proximity among services that belong to the same grouping while coming from different countries than the other way around. Within a given group, services share similar institutional routines and relations to technology. It is noticeable that the introduction of high volumes of data is having a strong transformative effect on the interior-centred services, which previously were relying much less on this kind of tools. This has become a challenge from both a technical and economic perspective: a quarter of justice expenses are now caused by payments to operators to compensate for the cost of accessing data. He concluded by stressing that the characteristics of the people who work in the services have a defining role on the “practicing spaces” (espaces de pratique) and on the possibility of collaboration, which is consistent with the typical Bourdieusian approach that is based on both position and disposition.

Second panellists Bernard Voutat and Hervé Rayner used a scandal that happened in Switzerland as a case study to understand what is the basis of (de)legitimation of intelligence services. They indicated that a scandal can develop when three ingredients are simultaneously present: public denunciation, multisectoral mobilisation and changes in the perceptions of what is possible. Until the end of the 1980s, the Domestic Political Intelligence (Renseignement Politique Intérieur: RPI) was seen as legitimate and operated without legal constraints. Its actions were mainly directed towards Communist groups. However, in what would be known as the “secret files scandal”, it was revealed in 1989 that 900,000 files had been constituted on Swiss citizens and stored in Bern. Consequently, mobilisations started against the “snooping state”, including street protests. 350,000 people demanded access to their personal files and 30,000 complaints were filed, which was revealing of the judiciarisation of the controversy. However, only five of them eventually led to an indemnisation.
From the political side, the government used denials or euphemisms when dealing with the exposed practices, an investigatory parliamentary committee was set up and six-year long legislative process took place to establish a legal framework for the services activities. The re-legitimation process of the RPI was based on a discourse of “constraints specific to today’s liberal democracies” (in Dobry’s words) rather than a vertical logic articulated around the “rule of law” concept and values matching the citizens’ beliefs.

Third panellist Jean-Paul Hanon presented how intelligence circulates in Germany, an issue of particular relevance in a very decentralised system: each land has its own police, with its intelligence division. The information collected at the federal level and from the länder is directed to a platform called “INPOL”, which is also equipped with automated information-processing capabilities. However, the local agencies retain the right to decide whether to share this information or not, and to restrict its use. The BKA (interior intelligence service) is the main administrator of the platform and it plays a liaison role with Interpol, Europol and foreign countries. A push is already underway to develop its cyber capabilities, with the recruitment of 1,500 new agents in this area by 2020. The BND (exterior intelligence services) has direct access to INPOL and it is the prime destinatory of terrorism-related information. Its selectors are defined jointly with the NSA, or by the NSA itself. Secret services have access to all police information, but information flows in the other direction are subject to stricter conditions. In short, Jean-Paul Hanon underscored that the existence of different levels of data collection (locally, nationally and with foreign third parties) are no impediment to data circulation, thanks to the interconnection of platforms and their processing capabilities. His analysis of the laws that have been approved in relation to intelligence reveal some patterns, such as a widening of the competences of the police and intelligence services, the central role granted to technology in their labour and the destabilisation of the traditional balance between liberty and security: the law appears to follow the demands of the services, leaving little weight to the Human Rights considerations. Instead of regulating the services’ activities, the German law appears to act as a powerful vector for their autonomisation, in particular in front of parliamentary control.

Fourth panellist, judge Gilles Sainati highlighted the similarities between the French and the German situations regarding the empowerment of intelligence agencies. From his experience, he asserted that the provocative question about whether there is a “programmed obsolescence of the judge” deserves to be seriously posed. He observed that several trends make it easier and easier to bypass the restraints imposed by the law and the controlling role exercised by the judge. The presumption of innocence has ceased to apply in practice where mass surveillance is practiced. Likewise, the principles of proportionality and speciality, essential in criminal law, have been “exploited”. Nineteen security laws have been adopted in France since 2000 and have generalised what was supposed to be measures of exception. The use of interception tools has become extremely common and directed towards a wide circle of people, to include the suspect and anyone they are in contact with, even in the preliminary stage of an investigation. Only in the judicial realm, 600,000 interceptions of phone communications and 400,000 text messages take place every week. The economic cost of such practices is heavy: the resources affected to them imply that other dimensions of the court activity become harder to finance. Vaguely defined terms, such as “terrorism” and “organised group” (bande organisée) allow to considerably expand the powers of law enforcement and intelligence services: the control of the criminal qualification takes place a posteriori and, should such qualification be modified at a later stage, the evidence collected under the original qualification will not be discarded. The explicit inclusion of a “prevention” objective in the 2015 Intelligence Law “against threats to the life of the Nation” represents an additional step in the same direction and allows to use highly intrusive techniques against peaceful militant groups. Both the technologisation and the generalisation of incontrolable professional practices further complicate the labor of the judge as a guarantor of the legality of the proceedings.

Finally, fifth panellist Anthony Amicelle presented the role of “financial intelligence services”, which are in charge of tracking irregularities in financial flows. Their number has grown
exponentially worldwide in the past three decades: from none to over 180 now, and they are sharing
information with one another. France was spearheading this trend with the creation of TRACFIN
in 1990, whereas in Canada FINTRAC was created ten years later. Focusing on this latter country,
the speaker notes that, at first, the process consisted in the body detecting financial anomalies and
forwarding them to the relevant authorities, which was consistent with the stated initial objective
to “lead” and “orient” intelligence and policing practices. However, they were often met with a
lack of interest from their partners, since this information was not meeting their current priorities.
Therefore, while the financial agency considered its “informational capital” as a strength, it was not
valued as such by the other services. Five years later, FINTRAC reversed the logic, by first asking
them what their concerns were, and then launching investigations in this direction, in a reactive
approach that contrasts with the proactivity shown by TRACFIN. The way the collected
information is presented is also adapted to the needs and rationalities of the recipient. This is the
way the Canadian organ has been able to build its previously deficient legitimacy in the sector, at the national level.
An undesired consequence of such a way to proceed is that FINTRAC has found itself associated
with the public legitimation of certain priorities, chief among them is the fight against terrorism. It
contributes to confirm it as a priority, despite the fact that, in financial terms, it represents a very
tiny percentage of all irregular flows.

In his comments, Francesco Ragazzi highlighted the analogies used to refer to the networks,
comparing them with water tubes (Jean-Paul Hanon) or a market (Anthony Amicelle) and raises a
series of questions to the different speakers. Laurent Bonelli clarified that the “multiple
correspondence analysis” used in his research has a pedagogical rather than revealing role, that
allowed him to expose the relevance of underestimated variables, such as having agents on the
ground or not. Jean-Paul Hanon clarifies that in Germany, evidence obtained through intelligence
services has no legal value before a judge. Gilles Sainati indicated that the international cooperation
is very limited for ordinary criminal cases, but much more advanced when it comes to terrorism.
He has witnessed only a few requests of information directed specifically to “GAFAM” companies
and stressed the complexity of such a mechanism.

The fourth panel focused on intelligence operations and human rights infringements. Key
questions were centred on how to frame the limits in democratic regimes, whether national
oversights are strong enough and what a transnational model of oversight could look like in case
of joint intelligence operations.

Panellist Elspeth Guild began with the Big Brother Watch v. UK judgment from 13 September 2018
in which the ECtHR essentially accepted bulk surveillance as a practice carried out by states. It also
stated that when mass surveillance is conducted, adequate guarantees of safeguarding rights should
be in place, as well as supervisory control. The Court recognised that surveillance by definition
interfered with the right to privacy. The right to privacy is a gateway right in international law
through which other human rights can become violated if it is infringed upon. It can lead to harmful
consequences for democratic society as a whole, impose a chilling effect and infringe upon the
right of freedom of expression. Should the Court have been harsher in its judgment? It put the
responsibility on oversight bodies rather than suggesting any involvement on its part. Oversight
bodies can provide mechanisms of control and supervision. However, the central question remains:
Oversight of what? What exactly is the purpose against which oversight can check if violations are
justified? Different reasons given to justify mass surveillance, such as terrorism or serious crime,
national security etc., have a varying and broad definition. Another central problem is the citizen/foreigner
distinction in mass surveillance, where foreigners are seen as ‘fair game’. It is also unclear who exactly should
be overseen. As indicated in the Big Brother Watch judgment, there are nine agencies in the UK that
conduct mass surveillance, while only three are generally talked about (GCHQ, MI5 and MI6).
Moreover, can this responsibility of oversight be shared transnationally with other oversight
bodies? And who precisely should conduct impartial oversight? Would multiple fora be a solution with independent supervisors and judges, parliamentary committees and technical experts? All these are central questions which are yet to be solved.

Second panellist Félix Blanc focused on extraterritorial intelligence and global oversight, with a particular focus on the infrastructure of telecommunications, submarine cables and how precisely access to data is enabled. The Snowden disclosures revealed PRISM and Upstream as central programmes cooperating with private partners such as ATT and Verizon. Within this context, submarine cables are crucial for Internet infrastructure as well as for the conduct of mass surveillance. They also constitute the nexus between intercontinental communications and terrestrial cables. Historically, they follow the telegraph system of the 19th century established by the UK, France and the US who occupy a dominant position in this network. He points to the central importance of interconnection points as central nodes, such as the nodal point in Marseille, which connects 300 Internet providers. Bulk collection of data is precisely made possible through these points. Oversight might not be enough in this geopolitical struggle for transnational intelligence collection and instead a system of checks and balances should be introduced.

Panellist Kilian Vieth addressed the issue of legal safeguards and oversight. Against the background of the EctHR judgment in the Big Brother Watch case, how can oversight be improved? Together with Thorsten Wetzling, he published a report on good practices of oversight, based on the study of various oversight bodies. In the report, they identify several dozen such practices, including: 1- The end of the discrimination based on citizenship: The Netherlands introduced legislation which ended this distinction, showing how a more moderate intelligence law is possible. 2- Different intelligence oversight bodies are cooperating and provide advocacy reviews of foreign cooperation partners, and regularly disagree with official reports. This points to a strong position of these oversight bodies. 3- Instances of restriction of surveillance do exist, especially with regards to purpose limitations.

Finally, Rob Walker made sense of these issues from a political theory perspective. How precisely can a more general significance be derived from these details and array of practices? He historicises some of the central concepts which are at stake in these debates, notably the notion of ‘human’, liberty, necessity and security. Liberty in particular is the primary value of modern politics. How can it be combined with the alleged necessity of security, or with violence against others? Surveillance should be studied not as a security issue, but as an issue pertaining to liberty. How exactly can limits be imposed in liberty, and why a balance between liberty and security cannot be struck as an equilibrium? How can a new form of political imaginary emerge in light of the discussions of transnational oversight, challenging the notion of national oversight as not strong enough? In this context, it is important to engage new categories which deal with the unknown and go beyond these central distinctions such as citizens/foreigners, norm/exception, law/territory which have defined international politics for centuries.

In his comments, Valsamis Mitsilegas pointed to some of the central challenges raised by the panellists, notably on the actors involved in oversight. How can independence and competence be ensured, especially when boundaries have become increasingly blurred? Furthermore, time in surveillance plays a crucial role, in particular since bulk surveillance in real time has been legitimised through giving access to real time data. Another issue is space and the territorial reach of jurisdiction. Data itself has no nationality or territory, and yet legal responsibility is bound by the territorial state. Lastly, by focusing on oversight, are we losing track of questions of bulk surveillance as such and its legitimacy?

Philippe Bonditti underlined the important question surrounding the lack of definition on what the purpose of surveillance is and who precisely should conduct oversight. The transnationalisation of
intelligence suggests new forms of practices by intelligence agencies and new modalities of cooperation between lawyers, resulting in struggles which are waged domestically or transnationally. How precisely does this affect the practices of sovereignty by states?

**Book Launch: “Antiterrorism and Human Rights” by Elspeth Guild and Didier Bigo**

The final session of the day launched the recently published report ‘Anti- & Counter-Terrorism and Human Rights in Europe’ with comments by Kurt Graulich and Laurent Bonelli. Kurt Graulich’s remarks focused on the defence of democracies against terrorism and the rule of law. Anti-terrorist and even more counter-terrorist logics in their claims to defend democracy by protecting people and states often go against the core of the principles and universal self-understanding of democracies, promoting emergency and routinisation of exceptional rules. Terrorist attacks have to be combatted. However, fighting terrorism without an agreed-on definition of central terms poses severe legal problems. The case of Germany shows how a shift in the German Basic Law (Grundgesetz) occurred in 2006, giving the Federal Police Office the right to deal with all questions concerning terrorism, while before it was dealt with under the authority of the 16 regional police offices. In terms of a human rights perspective, Kurt Graulich argued that the main burden of protection does not lie on the Court in Strasbourg but is firstly a domestic responsibility.

Laurent Bonelli pointed to the fact that the report takes human rights as an inherent part of the rule of law as a point of departure. The report shows what is at stake with regards to human rights and counter-terrorism practices. The report takes a deliberate socio-legal perspective to human rights rather than philosophical and points to the uncertainty of the definition of terrorism and its political and legitimacy implications. Moreover, it places this central tension of human rights and terrorism within a sociology of the state. Terrorism targets the social and symbolic order guaranteed by the state, and thus the state perceives terrorism as a threat to its national order. Security professionals use precisely these threats to shift the purpose, while some court rulings, judges, and citizens resist. This creates a configuration of different actors that cannot simply be described as a single movement. The report therefore offers a pertinent analysis, but also some guidelines on how to better protect the rights of individuals. Lastly, it raises questions about the amalgam of migration and terrorism and whether or not it can be reversed.

**DAY 3: INTERROGATING THE RIGHT TO PRIVACY AND THE LIMITS OF SURVEILLANCE**

**Introduction & Panel 1: ‘Domestic Surveillance and European Courts’**

The third day marked the encounter of experts that had not yet come together to discuss the central issues at stake in a truly interdisciplinary setting. This day focused on emerging standards from two European Courts, the European Court of Human Rights and the European Court of Justice. Building on the previous panels, central issues to address are the foreigner/citizen distinction, technological developments and their difficulties to assess, and the impact of most recent Big Brother Watch judgment which emphasises supervision and oversight and the importance to develop a set of rules. What precisely are those rules? First, those regarding domestic surveillance vis-à-vis the right to privacy, the EU right to privacy and the EU General Data Protection Regulation. Second, those regarding external surveillance and the activities of intelligence services outside their own domestic territories. Third, regarding biometric data and the Internet.

How are the two courts dealing with sensitive data? Does metadata qualify for the same level of protection as content data? It is worth dealing with these legal questions when intelligence services do not usually engage with such legal questions, as they simply ‘do their job’? It is crucial to show to these officers that the law is not their enemy, that data protection and privacy rights are worth
pursuing and enable them to perform their functions in the best way without risks of liability. In light of these considerations, the first panel dealt with the following judgments: The Zakharov and Szabó judgments of the ECtHR, and the Tele2 and EU Canada PNR judgments of the ECJ.

As panellist Lorna Woods explained, claimant Zakharov is a journalist and issued proceedings against Russia after finding a black box plugger in the mobile network, allowing access to telecommunications data. This case highlights the blurred distinction between bulk and targeted surveillance. The claims were made based on Art. 8 of ECtHR (protection of personal data), highlighting an individual case of interference. The laws in Russia that set up this system were inaccessible and hence no effective remedies were in place. The ‘victimhood’ question is important with respect to whether surveillance was conducted in the context of bulk or targeted surveillance. Secret surveillance cases like this blur the category of victim/intrusion. How can the impact of generalised surveillance be assessed? The court eventually ruled that Russia’s legal provisions on surveillance did not provide adequate safeguards against arbitrariness or abuse, and hence violated article 8. Panellist Jean-Philippe Foegle assessed the ruling and its requirements with regards to data protection. The ruling shifted its emphasis to fairness rather than questioning whether data should be collected at all. Central requirements are now its lawfulness, oversight, safeguards and effective remedies.

Panellist Máté Dánél Szabó, one of the applicants of the case, examined the Szabó case. Within Hungarian law, the legal conditions of secret information gathering by intelligence services are unsatisfactory and there is no effective control of the application thereof. Secret information gathering for national security purposes is subject to ministerial authorisation, and there is no adequate posterior control or redress mechanism. No adequate institution, nor sufficient procedure exist in Hungary that would control the vaguely defined conditions. This lack of effective control of secret information gathering goes back to the nineties. Szabó was triggered by the 2011 amendments on the counter-terrorism body (i.e. Counter-Terrorism Center, TEK) which has been vested with the power of secret information gathering. The claimants, who are two lawyers working for a public watchdog NGO, filed a constitutional complaint to the Hungarian Constitutional Court based on the infringement of their right to privacy by the potential conduct of surveillance without the adequate guarantees. The Hungarian Constitutional Court dismissed the claimants’ complaints. Subsequently, they initiated the proceedings before the ECtHR and alleged the violation of their Article 8 ECtHR rights on the ground that they could potentially be subjected to unjustified and disproportionate surveillance without judicial control. The Hungarian Government put forth four arguments in respect to the issue before the ECtHR: The first argument was that domestic courts are incompetent to define the necessity of secret information gathering as they have no access to relevant data; the decision to conduct surveillance is political rather than legal, and the law affords a wide margin of appreciation to the Hungarian Government. The second argument was that it is impossible to specify exact criteria for secret information gathering and therefore a judicial decision would not have sufficient grounds. The decision to conduct surveillance is political and not legal and therefore a politician rather than a judge should make the decision. The third argument was that experience shows that judicial control is not more suitable than the governmental supervision. The fourth reason was that a parliamentary oversight body is in place and hence there are no signs of arbitrariness. The ECtHR ruled that safeguards in general have to be in place and that even though the judicial authorisation is not necessary, the authorisation of surveillance must be given by a body that must be independent of the executive power. At least the supervision of the authorisation should be judicial. Thus the judicial authorisation, or at least judicial control over the authorisation should be the main rule. The ruling, however, was not clear on whether oversight should be in place a priori or posteriori. Any blurred requirement in Szabó on the involvement of a judge is counterproductive because it allows the Hungarian Government to involve a domesticated institution. In fact, in view of the Government, the judgment means that judicial authorisation is not an absolute requirement and post factum control mechanism can substitute the a priori authorisation as a minimum standard. Szabó said that this interpretation by
the Government allows the non-independent authorisation of surveillance if an independent body controls it after the application of surveillance. Szabó underlined the importance of the independent decision making in the authorisation phase. If there is an ex-post control mechanism that involves an independent judge who can at least order to stop the ongoing activity, prior authorisation of surveillance conducted by a non-judiciary body would be acceptable. The secret nature of the surveillance and its irreversibility restrict freedom similarly to personal physical freedom. In order to avoid the total defencelessness of the individual, the law must guarantee the prevention of complete disregard of the interests of privacy. Because of the secret nature, the individual can challenge the legitimacy of the use of such measures only after it is finished. Therefore, the control mechanism is effective in the individual case only if it is automatic: a judge automatically reviews the decision (if it was made by a non-judicial body). Taking into consideration the level of intrusion, the post factum review (that is made after the surveillance was performed) is important but insufficient: autocratic governments can get the information regardless of whether later this practice may be judged as illegitimate.

Panellist Susie Alegre further analysed the Szabó judgment, and more generally the nature of safeguards proposed in this judgment. Can the law really keep up with the practice of surveillance, its technological developments? How much detail is needed in the law and how can law be accessible? Can mass surveillance ever be necessary in a democratic society? Is it a proportionate response? The judgment did not deal with these questions or offer guidelines. With the potential for error, how do we approach ‘collateral damage’ within privacy? Furthermore, the role of judges as independent actors is not clear, since they might not be aware of the impact of their authorisation. Perhaps a hybrid oversight mechanism might be of more use, involving juridical and technical experts. Could an oversight mechanism ever deny authorisation, and if not, what is the use? Lastly, we may look beyond privacy to the rights to freedom of thought and opinion including the right not to reveal my thoughts or opinions, the right not to have my thoughts or opinions manipulated, the right not to be penalised for my thoughts. While the right to privacy can be limited, the right to freedom of thought is an absolute right and can never be limited.

Panellist Orla Lynskey dealt with the Tele2 judgment and pointed to the importance of the 2002 e-Privacy Directive which stipulates the confidentiality of electronic supplies. Art. 15(1) of the Directive defines data retention as an exception to this general principle. In 2006, the EU enacted a data retention directive across its member states. Digital Rights Ireland challenged these data retention practices before the ECJ, which ruled in 2014 that the data retention directive was invalid due to the violation of the EU Charter rights to privacy and data protection. The central questions emerging from this case are: First, are data retention practices ever compatible with the Charter? Second, are the conditions set by the ECJ in the Digital Rights Ireland case mandatory or merely descriptive? The ECJ first recognised the admissibility of the case, and therefore its competence to oversee national data detention regimes. This could not be taken for granted beforehand, since art. 1(3) of the e-Privacy Directive states that it shall not apply to the activities concerning public and state security. It argued that art.15(1) of the e-Privacy Directive allowed for EU oversight on such practices by member states, by setting certain conditions to be met when interfering with the rights proclaimed in the document. About the first question, the ECJ concludes that the data retention regime does not violate the “essence” of the right to privacy (with an argument that appears to contradict the assertion, in another part of the same ruling, that metadata are not less sensitive than content) but that serious crime does not justify, in itself, mass and indiscriminate data retention. The Court rejects the idea that data retention becomes the rule rather than the exception, therefore admitting its existence under specific restrictions. Regarding the second question, there is still some ambiguity, but the ECJ did not explicitly present the requirements from the Digital Rights case as mandatory. What is worrisome in the Tele2 ruling is that the Court admits that data retention circumscribed to a certain geographical area would be lawful, which could be even worse than the general and indiscriminate practice, for the discriminatory impact it would have on the targeted populations.
The panel then moved to the ruling about the EU-Canada PNR agreement, with Elif Mendos Kuskonmaz as the first speaker on this topic. While the transmission of passenger name records from the airlines to the authorities was made on a voluntary basis since the 1990s, the USA converted this information-sharing into an obligation after 11/9/2001. The companies found themselves in the middle of two contradictory legal requirements, since the EU applies strict data protection requirements. After the previous agreement expired in 2009, EU and Canada opened negotiations for a new one but in 2017 the ECJ ruled that the envisaged document was not in line with the EU Charter of Fundamental Rights and should be re-negotiated. It also found that it was not based on a proper legal basis, since it should not be only under judicial and police cooperation but also under data protection. A worrisome aspect of the ruling is that whereas the use and retention of the data can only take place for individuals that are identified as representing a risk, there is no such restriction regarding the transfer of such data, which can take place in a general and indiscriminate fashion: it therefore represents a step back in terms of the EU Charter standards, in comparison to the rejection of such a logic in the Tele2 case. The speaker also questions the proportionality and appropriateness of the PNR scheme itself in comparison to the magnitude of the threats it is supposed to fight against.

On the same subject, Arianna Vedaschi admitted that there is some bad news - mass surveillance in itself is not deemed unacceptable - but she emphasised the good ones, which have to do with the very high standards that the Court demands, in order for the system to be considered compatible with articles 7, 8 (right to privacy and personal data) and 52 (principle of proportionality) of the EU Charter. Among the reasons that the ECJ used to dismiss the projected agreement are:

- the lack of clarity regarding the purposes
- the extensiveness and unbounded nature of the type of personal data requested
- the potentially unjustified collection of sensitive data, even in the name of the fight against terrorism
- the fact that profiling is forbidden by the Court
- the continued retention of data, in particular once passengers leave Canada
- the risk of circumvention of EU rules if Canada transfers data to third countries
- the absence of notification
- the absence of a fully independent oversight body

This list permits to infer that the conditions to be met are quite strict and reflect the Court’s intention to strike a balance between data protection and security needs. Arianna Vedaschi explained that the Court may well be admitting surveillance in theoretical terms while imposing conditions that would make it impossible in practical terms. Through the Court, the EU is playing a leadership role in the field of data protection.

In his comments, Professor Kurt Graulich underscored how the “Zakharov” name was associated with the defense of human rights. He stressed that the ECtHR allows to remind the importance of human rights standards in “modern forms of personal regimes in so-called democracies”. Concerning the Tele 2 case, he argues that the EU has no competence regarding data retention and he qualifies as “nonsense” the application of conditions on something that is inherently unlawful, which he underscores by quoting Theodor W. Adorno: “there is nothing right in the wrong”. He is very vocal against the notion of compulsory data retention by companies, for purposes that are distinct from the operation of their businesses: he compares such a regime with the hypothetical obligation on individuals to store litter for a certain amount of time and/or write diaries for any future need in the context of an eventual investigation. From his perspective, both European Courts are on the wrong track.

In the Q&A session, Lorna Woods indicated that it would be difficult for both Courts to outright reject mass surveillance when the states are pushing so strongly in this direction, this is why both
have chosen the path of applying harsh conditions to such practices. However, she considered that both Courts have overlooked the volume of information that the governments are now able to collect in our hyperconnected world, and that this is a “gap” in their proportionality assessment. Should anything be allowed providing there are sufficient safeguards? Orla Lynskey expressed worries that the effective use of data obtained through surveillance in future judgments may be legitimizing their collection in the eyes of the public opinion.

Panel 2: ‘External Surveillance and European Courts’

Moving from instances of domestic surveillance, the second panel focused on cases of (foreign) external surveillance and pending litigation before the ECtHR and the ECJ. This form of surveillance extends beyond the jurisdiction of the state and covers inter-state cooperation to share personal data and state-private sector arrangements for personal data sharing in a transnational setting.

Panellist Kurt Graulich focused on the Weber & Saravia case before the ECtHR. He argues that this case can be seen as a meta case as the ECtHR decision came after the decision of the German Constitutional Court on the same issue. He lays out the legal and factual conditions: The law concerned is Article 10 of the Basic Law (Grundgesetz), enshrining the freedom of telecommunications. The law which allows a restriction of this article was made during the Cold War in 1968 and restored after the reunification in 1994 where lawmakers increased the range of the law. The purpose changed after the Soviet Union broke up and focused on organised criminal gangs, and thus required a widening of the scope of the competence of the foreign intelligence service. In this light, how can the freedom of telecommunications be ensured? The law only concerns cross-border telecommunications and a complaint was made to the German Constitutional Court, cancelling parts of the law which were not in the competence of the Federation. But what was important for the ECtHR decision that followed was the Court’s remarks about the adequacy of safeguards that were in place. In 1968 the G10 Commission was founded which was a commission between the court and parliament who worked independently and efficiently. After the sentence in Karlsruhe the two claimants appealed to the ECtHR, which ruled in a similar manner as the German Constitutional Court and highlighted that data retention was in accordance with the constitution because there was a legal base and enough safeguards in place to provide adequate control over the scope of surveillance.

Panellist Lorna Woods focused on the Big Brother Watch ruling. The case includes three challenges in the UK which were joined, by ten Human Rights Organisations, the Bureau of Investigative Journalism and Alice Ross who all raise slightly different issues. The Court’s assessment considered post-legislative changes and cases after Snowden which revealed new information. The central question is the impact of the Big Brother judgment for internal, bulk surveillance but also for distinct targeted surveillance. The Court attempted to derive common principles from this carried and fragmented landscape. With this in mind, is the judgment really solely about the external context? About bulk or general surveillance? The Court did not base its reasoning on the fact that they dealt with foreigners and dismissed claims of discrimination of treatments. Bulk interception was limited to external communications which is a very broad idea, as for instance Facebook or Google users’ data could potentially go to servers outside their own country. Furthermore, the judgment made two distinctions: One between content and traffic data and the other between acquisition and examination of data. The Court confirmed that bulk interception was not impermissible as long as safeguards were in place. Moreover, the Court did not look into the question on where and how data interception is taking place, or at the exit of data from the UK. Is the law on data sharing really as clear as assumed? Generally, is there an essence for the Court of Article 8? It has not yet been found in the context of surveillance. Moreover, the predictive use of mass datasets has not been addressed at all.
Third panellist Jeremy Heymann looked at the Schrems ruling of 2015. Schrems, a PhD student on data protection and an activist, has been filing claims against Facebook and its failure to protect personal data all around Europe since 2010. The proceeding started when Schrems filed a complaint against the data protection commissioner of Ireland because he claimed that Facebook Ireland was transferring personal data to the US, which could then be accessed by the FBI, NSA and other agencies. According to the data protection commissioner the complaint could not be filed as there were no proofs that the NSA was actually collecting data. This raises a very interesting question within private law, where the burden of proof question in the protection of personal data lies with the claimant. How exactly can someone prove that government agencies have access to personal data? How can data flow be proved? Thanks to Edward Snowden’s leaks, the connection between access to personal data on Facebook and its transfer to the NSA could at least be envisioned as possible. The context of the case was the Safe Harbour agreement between the EU and the US, which was based on the assessment that the US had adequate safeguards in place and could therefore be provided with data from the EU. The Court ruled that in fact the Safe Harbour was not safe. Another agreement would have to be proposed. Privacy Shield from 2016 is such a new agreement, but still flawed. In the US, companies can simply self-certify that they are complying with the protection of personal data, which makes this a questionable safeguard. He concludes with three points: First, a BCG study showed that the market value of the digital sector is about 1,000 billion euros, which allows to put in perspective the level of the fines to be paid by private companies. Second, users need to know the outcome of data flows, where the data is stored and who it is transferred to. Last, the ambit for protection by the law is not clear, especially in a global context where counter-statutes can be issued and a fragile balance between different legislations needs to be struck.

Fourth panellist Elaine Fahey looked at the Schrems judgment from the perspective of international relations and the history of transatlantic relations, which can be characterised as a series of failures and successes in the same breath. The mutual sharing agreement was a brief success before Schrems took on the US government in the name of a vast number of private consumers. The Schrems 1 ruling was a really long decision with clear reasoning. Moreover, it enshrined Schrems as a data warrior and the right for him to be a public interest figure. The case itself draws together an uneven mix of parties and defends his position as a citizen-consumer and advocate. Another central question to be considered is the role of US law and how much of it should be considered. The case shows how quickly the rules of the game change.

Panellist Rudi Fortson examined the Big Brother Watch judgment and its implications for the UK. When looking at the issue of public perception after a terrorist attack, it becomes evident that the media immediately asks whether the suspect can be identified, and whether the person was on the radar of the police or intelligence services. There seems to be a larger expectation from the public point of view that law enforcement should carry out surveillance to prevent the commission of crime. The Big Brother Watch Case states that it is legitimate for the Court to take a firm stance against global terrorism, and the flow of information between security services of many countries in all parts of the world is necessary due to the complex nature of global terror networks, provided that adequate safeguards are in place. In the case of the UK, the same applies to serious crime more broadly. The traditional English approach to the law is that unless certain conduct is explicitly prohibited, it is allowed. With regards to surveillance, the UK is now catching up with the European approach which regulates the conduct by law. The Big Brother Watch case might indicate a shift towards the UK and US positions, looking at procedure, form and then a large number of caveats are woven into it. Despite establishing a set of legal rules, does the law really provide effective protection to individuals subject to surveillance, and does it provide effective remedies? What form does judicial oversight take? There is a march towards gathering data on an enormous scope and processing it, how can this be justified?

Panellist Elif Mendos Kuskonmaz focused on the EU Canada PNR case. She analysed what exactly the data processing mechanisms and measures are in the context of border control and external surveillance.
What happens to rights under EU law once data is transferred and the external context comes in? The PNR data transfer is given green light by the Court although there is no evidence to what extent it actually helps fight terrorism. This case shows how a data-driven society and border controls shape the conduct of counter-terrorism, where border control, law enforcement and intelligence become merged. What exactly is the impact on privacy protection and freedom of thought? If the purpose is to identify people who are crossing borders, Advanced Passenger Information, which is a digitised version of the passport that is created and sent in advance of boarding to authorities can exactly do that. The purpose of this form of data retention becomes ingrained in a grey area. It is not only about surveillance but also how the counter-terrorism purpose transforms border controls and affects people’s privacy.

Panellist Ricardo Rodrigues de Oliveira raised two general points for the panel concerning external surveillance. The PNR agreement that regulates the transfer of PNR data from EU to Canada is not exactly a peer-to-peer relation, but a private to public one. This points to a complex relationship within the security assemblage and raises concerns about the number of people who have access to personal data and potentials for leakage, which the ECJ did not address. Furthermore, the access to data by Canada should be dependent on prior review or an independent administrative body. However, the practical consequences of trying to lead law enforcement and counter-terrorism with prior review might not be feasible, something which has to be rethought. He pointed to two findings of the ECJ. First, the agreement allows for systematic and continuous transfer of data of all passenger flying between the EU and Canada (amounting to 2-3 Mio. people in less than a year). Around 300 persons have been detected, detained and prosecuted under this system. This numerical discrepancy is not weighed by the Court but merely presented. Second, the GDPR, which the panellist claim is anything but obvious and clear, provides a higher level of protection of fundamental rights, but does it apply in the context of PNR? The Court does not tackle this issue. In sum, the ECJ allows the PNR scheme in general to remain in place, since only details are objected.

In his comments, Théodore Christakis further built on the continuity between domestic and external surveillance, quoting a recent headline on several UK intelligence agencies admitting to unlawfully spying on Privacy International, collecting their private data and examining it. This is a striking admission because surveillance is usually justified based on the threat of terrorism, and hence this showcases the risks of mass surveillance. He first pointed to a clear difference between the two Courts (i.e. ECJ and ECtHR), where it appears more flexible in the PNR judgment compared to the Tele2 judgment where it went too far. The ECJ is following a path which is clearly requiring a very high standard, agreeing to mass surveillance but with oversight and control. This is nothing new in itself, but how can this control be exercised? Luxembourg clearly underlines the strict necessity test as necessary and offers little margin of appreciation to states, posing strong requirements of control on all levels. In the Szabó judgment, the Strasbourg Court endorsed the strict necessity test underlined by Luxembourg. This points to a possible harmonisation between the two courts. In light of this, the Big Brother Watch judgment seems to deconstruct some of their criteria laid out in previous case law, in particular with regards to notification which the ruling says is illogical in mass surveillance regimes. Théodore Christakis rejected this interpretation since, at a later stage, mass surveillance becomes targeted surveillance, at which point notification fully makes sense.

Panel 3: “Biometrics, Internet, and European Courts”

First panellist Niovi Vavoula analysed the S & Marper 2008 ruling by the ECtHR. This case is based on a complaint by two UK citizens concerning their biometric data (DNA samples, fingerprints) which had been collected and conserved indefinitely by the national authorities. Their demands to have them destroyed had been rejected. They argued that it was a privacy breach with ever-lasting consequences. The Strasbourg Court changed its previous stance from the Kinnunen vs. Finland case and ruled that such practice did not pass the proportionality test, in particular because of its indiscriminate nature: neither the gravity of the offense or the culpability of the suspect were taken into account. It also pointed at the stigmatising effect of an indefinite retention of such personal
data and stressed that the interference to privacy was effective since the collection stage, regardless of whether or how they may be eventually used later. Niovi Vavoula derived from the case a “toolbox” of specific limits on the retention of biometric data, which comprise: the necessary distinction between innocent and convicted people, the gravity of the crime, the age of the person, the possibility for removal, the existence of an independent review of the motives and fixed timespan for conservation. Article 9 of the GDPR specifically refers to the issue of biometric data.

Draw wider inferences from the same case, Evelien Brouwer stressed that the ECtHR, while explicitly recognising the importance of ‘modern scientific techniques of investigation and identification’ to fight crime and terrorism, explicitly underlined the obligation of states to exercise careful scrutiny of any state measure authorising data retention without the consent of the person concerned. The ECtHR addressed in that regard in particular the special responsibility of any state claiming a pioneering role in the development of new technologies. In S. & Marper 2008, the ECtHR also made clear that the general approach regarding photographs and voice samples as developed in the earlier judgment P.G. and J.H. v. UK should also be followed with regard to fingerprints, stating that ‘neutral, objective and irrefutable material’ is always capable of affecting the right to private life. Brouwer notes that while the ECtHR stressed the importance of the proportionality test, it did not address the question of effectiveness, and whether the collection and conservation of biometric data is useful at all to fight crime and protect public order, even if the applicants in this case explicitly questioned the reliability of the UK government’s claim to the success rate of the retention of DNA profiles of unconvicted persons. Finally, the explicit considerations of the Strasbourg Court in S. & Marper on the individual concerns about the possible future use of private information are important. This conclusion, comparable perhaps with the ECtHR’s warning against the ‘chilling effect’ of limitations to the freedom of speech, is particularly relevant considering the use and developments of extensive and interconnected databases and surveillance tools in the future and the fact that in some EU Member States the value of democracy and rule of law are currently openly questioned by national leaders.

Now moving to the Digital Rights Ireland ruling by the ECJ in 2014, Nóra Ni Loidean indicated that this case was key to assess the influence the ECtHR has on the ECJ: although Article 52(3) of the EU Charter obliges the ECJ to give the same meaning to the same sights as the ECtHR, this represents a floor, rather than a ceiling, meaning that a more extensive protection by the ECJ is still possible. She asserted that it was no coincidence that the ruling happened one year after the Snowden revelations and she qualified it as a landmark case that opened a chain reaction for other landmark cases. It was the first time that a whole directive was struck down under articles 7 and 8 of the Charter. It also raised questions about the consequences of such decision on the domestic laws about data retention. She further noted that the ECJ used principles that are clearly related to the landmark ruling ECtHR Amman vs. Switzerland of 2000 (where it was established that the collection of data and the subsequent use of it were two successive interferences) but did not mention explicitly that case: it rather used its own Rundfunk case of 2003. This marks a departure from explicit references to the ECtHR in the pre-Charter approach of the ECJ in its data privacy case law. Before the Charter, the ECJ was in the practice of routinely and openly citing the special significance of the ECtHR and the rulings of the ECtHR as a key source of inspiration for the general principles of EU law. Digital Rights Ireland highlights the intention of the ECJ to focus on the leading role of the EU Charter in the development of EU fundamental rights law.

Next panellist Marie-Laure Basilien-Gainche proceeded on the same case and highlights two points. First, about the “legitimate purpose” that the Court tried to identify, she raised the apparent contradiction regarding the objectives of the Data Retention Directive: formally, it has to do with the internal market while from a material perspective it is in fact focused on the fight against terrorism. She also wonders what level of “crime seriousness” would justify the use of retained data. Second, about the “guarantees of the adequate measures”, she lists the conditions that the ECJ identifies, in
addition to the “strict necessity”, in order to pass the proportionality test and therefore to preserve the fundamental rights:

- the subsequent exploitation of the collected data can be used only to detect and prevent “serious crime” (with the problem that this concept is still very vague and changing from country to country)
- The collection of data must be subject to a prior independent review (by a court as the best option by an independent administrative body) to assess the strict necessity of the access and subsequent use of the data
- the collected data must be stored in an EU Member State
- access to data must be limited to a restrictive number of persons, services, agencies in order to ensure the possibility of an in-depth control
- the retention time must be subject to certain limits depending on the kind of data.

Somehow, through this list the Court is inviting the national legislators, independent agencies and judges to take those criteria into account when designing or assessing the legality of each data retention regime.

Then the discussion moves to the 2014 Google Spain case, presented first by Jeremy Heymann, through which the ECJ proclaimed what would be known as the “right to be forgotten”. However, this designation is in fact abusive, since it would be better described as a “right not to be listed”. The case was won by a Spaniard who wanted his name not to be associated anymore in Google Search results with a story published in the mid-1990s in a newspaper, in which he was condemned for debt-related matters. The ECJ considered that Google was acting as a data controller and processor, and that its activity was falling in the realm of Directive 95/46 on the protection of personal data, which was therefore used as the main legal basis for the ruling. The most delicate issue regards the balance that has to be struck between the individual right for privacy and the collective right for access to information. In 2017, the French Council of State (Conseil d’Etat) made a preliminary question to the ECJ: what is the ambit and enforceability of such a right? In other words, it is about getting a “notice” about how to handle it.

Next panellist Orla Lysnkey underscored the fact that this ruling is the only one that is not as directly related to surveillance. She argued that this case provides an interesting clarification of the difference that exists between two close rights: it is a matter of data protection, but not “necessarily” an issue of privacy since there is not “always” a reasonable expectation of privacy for information that is freely available on the Internet. She considers that this effective use of the right to data protection is a “good thing” in front of this trend towards a data-driven society. Additionally, she observes that the reasoning of the Court made an extensive interpretation of key concepts in order to ensure the effectiveness of the right to data protection. For instance, in its rejection of an argument from Google, the ECJ argued that the status of data controller does not require to be able to have an objective knowledge of which data it handles are of a personal kind and which are not. Finally, she stresses the significant uncertainty that exists between the legal regime on data collection by the private sector and the one that governs subsequent use of this data by public authorities. Which regime would apply if a state decided to purchase data from Google, should it decide to start data-broker activities? This situation, hypothetical so far in Europe, is already under development in China. In such a dystopian context, the right recognised through the Google Spain ruling might well reveal to be highly relevant.

Now moving to the EU Canada PNR ECJ Opinion, panellist Arianna Vedaschi argued that in the tension between a security-driven (defended by the Council and the Commission) and a human-rights oriented approach (promoted by the Parliament and the ECJ), the former is gaining ground for at least two reasons. First, although profiling and the collection of sensitive data are prohibited, the combination of non-sensitive data allows to get the same result. The draft Agreement listed sensitive data and prohibited resorting to it. However, it did not cover situations where sensitive information can (actually) be inferred even by crossing non-sensitive data. Thus, the ECJ did not take into account that PNR data, if crossed and matched, can reveal sensitive data even without being such per se. For example,
information on food may reveal religion or state of health. Second, the “depersonalisation” of data, that “can” take place 30 days after collection is made along a “pseudonymisation” logic, which is a reversible process (for example when it is essential for investigative purposes), instead of real anonymisation. Pseudonymised data does not cease to be personal data, whilst anonymised data does. The Court’s analysis could have shed more light on these two aspects.

Talking about the same case, last panellist Ricardo Rodrigues de Oliveira argued that it is necessary to “embrace” the fact that technology is collecting more and more information from the people, and that this trend only getting more obvious in the future. Starting from this premise, he made a call to move away from “privacy” concerns and to focus on procedural rights instead, which is, from his view, the logic behind the EU Canada PNR scheme. He also argued that in the context dominated by terrorism-generated fear, it is inevitable that new legislation allowing for more collection of data are approved. He intended to defend his point by showing that the negotiations of a PNR agreement between the EU and Canada was a very long process, that was allegedly streamlined after the Paris and Brussels attacks of 2015 and 2016 and the adoption in April 2016 of the EU PNR directive. However, he recognised that the Court made the right decision when it considered that the purported agreement was not meeting the proportionality criteria, for being too “extensive” and vague in the kind of data that would be collected. He concludes by an invitation to fight the “little details” rather than the principle itself of mass data collection.

In her comments, Segolène Barbou des Places raised three main questions:

- What does all of this mean in real life? Beyond those landmark judgments, what do ordinary Courts say in ordinary life? Legal uncertainty can also be found in the evolution through time: what is not sensitive or dangerous today could turn out to be in the future.

- What to do with the loopholes, incoherencies and lack of clarity in the Courts’ reasoning? It creates blind spots that, in turn, are a source of legal uncertainty. The moral principles and priorities that are behind the judges’ motivation are implicit and remain “unpacked”.

- How to derive general principles from those rulings, when so many variables are involved? There are variations depending on the kind of data, on the characteristics of the persons, on the type of interference and the way data is processed, on the degree of sensitivity of the data, on the degree of seriousness of the action, on time-defined criteria, etc.

In the Q&A session, Marie Laure Basilien-Gainche wondered how an effective oversight can take place when so many players participate in the intelligence sectors of a given country, and when the information is, additionally, shared with intelligence services from other states. In reaction to Ricardo Rodrigues de Oliveira’s comments, several panellists described themselves as “alarmed” and took the floor to defend the importance of the right to privacy and the insufficiencies of a protection that would rely only on procedural grounds. They remind of the importance of taking into account what future use can be made of data collected at a certain time and point to the chilling effect that arises from the collection itself. It is also emphasised that the right to privacy is a platform right, necessary for the enjoyment of other fundamental rights. Niovi Vavoula also reminded of the ECJ’s upcoming Ministerio Fiscal decision, which can address the questions on serious crime in connection with access to data.

Panel 4: “Surveillance before National Courts”

The final panel was dedicated to the pending litigation before national courts on surveillance measures of certain states, inviting panellists to imagine a possible outcome. The panellists focused on the cases of the US CLOUD Act, the German BND law, the UK Investigatory Powers Act and the French 2015 Intelligence Act. In many of these cases, national constitutional courts have led the way, with striking judgments against mass surveillance.

Panellist Théodore Christakis focused on the USA CLOUD Act. The point of departure for this act was the US vs. Microsoft case, after Microsoft was given a request by the FBI to hand over a
person’s data which was located in Ireland. Microsoft argued that the law that required them to do so did not have an extraterritorial reach and that the FBI had to request it from the Irish authorities. The US Government argued that Microsoft could simply access the data on a computer from Washington DC, attempting to circumvent the extraterritorial nature of the request. The panellist argues that such an argument is illogical and that the location of data matters, as highlighted by the European Data Protection Body. This problem was resolved by adopting the CLOUD Act in March this year, allowing an extraterritorial reach of American law. From the point of view of US law, the problem was resolved, but not from the point of European law. A conflict of laws was possible if for instance Microsoft obeyed an FBI warrant under the CLOUD Act but violated the GDPR and local legislation. To resolve this problem, the CLOUD Act provides for a conclusion of bilateral agreements with some governments, the content of which remains to be imagined. The Commission proposal for a regulation and a directive on “e-evidence” would allow EU governments to access data from Internet Service Providers between ten days and up to six hours, as opposed to the previous ten months on average. This EU legislation would have an extraterritorial reach, putting Europe on the same level as the US during negotiations on the bilateral agreement. This was strongly criticised by NGOs due to the privatisation of law enforcement. Therefore, in order to avoid the conflict of law, a data sharing agreement is needed between the EU and the US. The US, however, is not willing to adopt such an agreement with international organisations, but prefers bilateral agreements with governments, due to fears that some states in the EU will not present necessary human rights guarantees. This puts enormous pressure on the EU to create a level playing field.

Panellist Kurt Graulich talked about the German case and a big number of complaints to the Federal Administrative Court with regard to press information against the foreign secret services. The famous Eichmann case in particular attracts such complaints, with the press assuming that the BND is hiding files. The complaints were not yet successful, because first, the archive right stipulates a particular period before these documents can be opened and second, the legal base for this information request is not clear, as there is no special press law for this request. Another type of request concerns individual information requests on whether people were surveyed by the cross-border telecommunications interceptions. Some of these lawsuits had been successful, while others weren’t. The most important case is currently pending before the Constitutional Court. Two years ago, a new law was passed for the BND, concerning the ‘Ausland-Ausland Überwachung’ (foreign-foreign surveillance), regarding the telecommunications interception performed outside Germany. The Constitutional Court will now have to give an answer on whether or not the German Constitution, in this case, has to be abided by when acting outside Germany.

Panellist Thorsten Wetzling looked at the processes and arising challenges of the biggest intelligence reform in Germany in the last 30 years concerning the foreign-foreign intelligence collection. The position of oversight bodies in place in foreign surveillance practices are questionable and the pending case before the Constitutional Court will shed clarity on the reach of the Article 10 law. The German authorities have created three different categories of data collection: ‘The rest of the world’, ‘EU citizens’ (with EU officials being granted better protection) and ‘German citizens and residents’ for whom this does not apply. Can the right to privacy be restricted? Simply because the collection of data is conducted abroad, this does not mean that some of the architecture might not be used on domestic territory. There are different intrusion moments which very well could happen on German territory and therefore can be challenged on Constitutional grounds. The categorisation of different data sets as mentioned is very problematic and might not be technologically feasible. Is there a good enough verification of the filters in place? Who exactly oversees the filters? This shows how this is as much a legal as a technological question. Regarding the oversight body, the current independent body, which is of administrative nature rather than parliamentary or judiciary, has not enough access to the selectors when looking at the case of foreign intelligence. Moreover, the G10 commission has not yet been reformed due to the pending question of how the right to privacy can be extended to non-Germans.
Panellist Lorna Woods looked at the case of the UK Investigatory Power Acts (IPA) and the Liberty ruling (UK High Court, April 2018). The background to this case is the striking down of the EU data retention directive in April 2014 by the Digital Rights Ireland ECJ ruling, which left the UK system with no legal basis. This led to DRIPA (July 2014) which was challenged in the Tele2-Watson ruling, and applied by the Court of Appeal after DRIPA had expired. This then led to the IPA (Nov. 2016) which with regard to the retention of telecommunications data looked remarkably similar to the regime that was criticised by the court in the Tele2-Watson judgment. Liberty tried to argue in the same vein before the High Court. The Court, which is lower in status than the Court of Appeal, was constrained by the latter and could not issue a different judgment, tackling European law in a questionable way. The panellist argues that something got lost in translation in these judgments. The English Court distinguished between that which the Court said with relation to the Swedish legislation (in Tele2) and that in relation to DRIPA. Therefore, if the UK is not directly addressed, it does not apply to it. The Privacy International case referred to the ECJ which then raised questions of national security, an issue the High Court cannot deal with. The Court instead moved to the issue of general and indiscriminate retention of data. In the case of the UK, the Secretary of State may issue notices on data retention and target a certain part of the population, which might still concern a vast number. However, the Court ruled that the Secretary of State made a choice with regards to proportionality of data retention and considered the impact on privacy. Furthermore, the question of notification was not dealt with by the Court of Justice, and the EU itself remained unclear about this point. The judicial review succeeded on points already covered in Watson, for the remaining points the Court has ruled against the applicant or stayed it, overall making this not a helpful judgment.

Panellist Marie-Laure Basilien-Gainche focused on the case of the French 2015 Intelligence Act. This act is part of an array of intelligence acts passed in the last three years in the French parliament, starting with the intelligence act from July 2015 which was passed in parliament after a fast track procedure. Another law was passed in November 2015 regarding international surveillance, and a third law followed in July 2016 prolonging the state of emergency in France, which authorised applying a normal procedure for targeted surveillance on meta data. In October 2017, an act regarding radio surveillance was passed. The surveillance disposal organised by such laws is very extensive, intrusive and permits mass surveillance of meta data. There are numerous, wide and vague grounds permitting this practice, such as: national defence, territorial integrity, major economic, scientific interests of France, the prevention of attacks, collective violence likely to cause serious harm to public peace, proliferation of weapons of mass destruction, terrorism, etc. A decree in January 2016 multiplied surveillance techniques and widened virtually all possible grounds to conduct surveillance. For instance, the expression “identified as a [terrorist] threat” is replaced by more sibylline one that is “likely related to a threat”. The law that was passed in November 2015 allows French intelligence services to conduct surveillance of global communications networks from French territory because it provides for the surveillance of ‘communications emitted from or received abroad’. Also, the current regime allows for bulk exploitation and data retention with reduced oversight because foreigners have lesser safeguards against these activities. French citizens are also concerned because most of the most of French residents’ online communications are “emitted or received abroad” – particularly in the US or in other European countries where the servers of the largest online service providers are located. French citizens as well as foreigners are affected by the current French legal order on surveillance, enacting a very worrying legal landscape with little legal guarantees, light controls, unsatisfactory redress mechanisms, which make it difficult for individual to bring a case and heavily relies on secrecy.

Panellist Félix Tréguer offered an insight into his work as an advocate, who has been part of a group of volunteers, legal analysts, and technologists who started working together in late 2013 on intelligence and privacy issues (la quadrature du net). After the first attempt to legalise the access
to metadata by the intelligence agencies in late 2013 (just after Snowden) appeared, the group worked on challenging the application decree. The goal was to implement the Digital Rights Ireland ruling in France. After this, the government introduced the Intelligence Act in spring 2015, and the group offered advocacy and analysis around the act, when Parliament adopted the act. After their brief to the Constitutional Council, providing an ex ante review of the Act, the Council struck down a provision on international surveillance through a secret decree which provided no details in the law of how international surveillance would work. The government had to put into law the whole authorisation measures. In late 2015, the government adopted the implementation decree of the Intelligence Act. The goal of the group was to attack this decree before the Council of State, with only two months to introduce their challenge. This was accompanied by a revelation in Le Monde (April 2016) on the spying on Thierry Solère, a MP who was a right-wing opponent of one of Sarkozy’s friends, in the 2012 elections. The French DGSE officials argued that this practice was legal as there was an old provision from a 1991 law, when the DGSE set up a satellite monitoring system, allowing them full discretion with regards to “radio communications”. There were no oversight mechanisms in place, encompassing any form of surveillance. This 1991 provision survived the adoption of the Intelligence Act. The panellist’s advocacy group introduced a question around this fact which led the Constitutional Council to strike down on the law. A last point concerns the technological aspects of analysing the collected meta data. During the state of emergency, over 4,000 houses were raided, where the law enforcement officials took data from all electronic devices but were unable to analyse it. The head of the DGSI argued that big data analytics were needed to make sense of it. However, the law does not provide for the authorisation of the DGSI to conduct big data analytics domestically, but only in the foreign context.

Finally, comments were offered by Jeremy Heymann, who observed that in the case of Théodore’s intervention, states still seemed to abide by the rule of law in the context of mass surveillance. The expositions about Germany, the UK and France, however, point to a different direction where the rule of law is only abided by in appearance. In practice, surveillance laws are very broad and blurred, and a very large margin of manoeuvre is left to the state. What does this entail for controls, judicial review and the respect for the rule of law? Another interesting comparison is offered between the case of Germany and the US, where in Germany, the issue of extraterritorial reach of the law is debated and raises concerns about the reach of the Constitution outside its domestic application. What can be an adequate response to this? For the US, there seems to be no problem about this issue of extraterritoriality. He further raises the question of where Europe comes in in the context of those domestic discussions. Mass surveillance on foreigners encompasses EU citizens, so how does Europe deal with this issue? Should the EU claim jurisdiction? This is an open question about collective or individual responsibility with no clear answers.