www.cybersecurity-liability.ch

CONFERENCE REPORT

INTRODUCTION

On June 20, 2019, over 100 participants attended the second Geneva Cybersecurity Law & Policy Conference titled *Cybersecurity: how to allocate liability*, held in the framework of a research project between the University of Geneva and the Hebrew University of Jerusalem (HUJI). For a second year, this conference aimed at presenting selected legal and policy aspects of cybersecurity in a crosscutting approach.

The conference opened with some introductory remarks from **Prof. Bénédict Foëx**, Dean of the Faculty of Law, University of Geneva, who noted that large-scale cyberattacks in the past years have unfortunately shown that damages of considerable scale can be caused in very short times. Yet, cyberattacks are still not well regulated especially when it comes to allocating liability. By having both academics and professionals from different industries as panelists, the conference intends to provide answers that will have an impact on the "real world" and ensure that issues are addressed from a holistic perspective.

Dr. Yaniv Benhamou, University of Geneva, pursued the introduction by indicating that the event is also part of the 6th edition of the UNIGE Internet L@w Summer School[1] and linked to the fourth Geneva Internet L@w Research Colloquium.[2] Questions of cybersecurity are becoming increasingly significant, as recent events have shown that any device and all infrastructures, including the critical ones, can be hacked. The objective of this joint research project with the Hebrew University of Jerusalem is to shake the legal foundations of cybersecurity in order to identify standards and determine who can be liable in cases of cyber attacks. The University of Geneva is also currently setting up a Center for digital law in the context of its Digital Strategy, thus ensuring to remain a leader in this field.

Dr. Benhamou further explained that the traditional perspective of cybersecurity viewed as involving only two actors – the cyber pirate and the cyber-victim – is too narrow. It has now become clear that attention should be paid to the entire cybersecurity ecosystem, which involves not only victims and pirates, but also clients, employees, boards of directors, information technology (IT) vendors, insurers, and even States – different stakeholders who may all have a role to play in cybersecurity liability issues. It should also be noted that today's hackers can wear either a "white hat" (performing "ethical hacking" by using their abilities for good, ethical, and legal purposes), "grey hat" (may sometimes violate laws or ethical standards without having malicious intent) or "black hat" (ill-intentioned hackers looking to cause harm), and are sometimes so organized that they have registered companies and employees, making it more difficult to identify them and hold them liable for the damages they cause. We also need to define the nature of this potential liability: is it criminal, civil, or both? Which already existing liability regimes may apply, and can they be cumulated? How to calculate damages? What is the standard of care? What is the role of data protection? How can insurance apply? What are the technical challenges associated with new technologies such as artificial intelligence (AI) when it comes to assessing liability? The University of Geneva's and Hebrew University of Jerusalem's joint research project hopes to analyze those issues in more detail and suggest some answers.

Elaborating on the role of AI in cybersecurity, Dr. Benhamou indicated that AI is increasingly used by companies to enhance their cybersecurity, but also hackers who use it to better penetrate their victims' systems. Although undoubtedly useful, AI-based methods in cybersecurity also bring their share of complications, which make it difficult to allocate liability in case of a problem. One of them is related to the high amount of input (data) fed into the AI system, which is then processed by algorithms and eventually generates output (new data). The way AI functions creates a so-called "blackbox" issue, because we do not always understand how AI processes the input and generates output. This can be illustrated with the example of a facial recognition neural network that scans people's faces and issues an opinion as to their ethnicity. In such a case, it is not always possible to identify which features were processed, the weight that was given to each feature in the global assessment, whether there are unethical bias in the processing, etc. Another example is the "Facebook chatbots" case, where Facebook stopped an experiment after two artificially intelligent chatbots, initially programmed to exchange in English and negotiate between themselves, started chatting to each other in a language only they understood.

[1] https://www.unige.ch/droit/pi/summer-schools/internet-law/internet-law-summer-school-2019

[2] https://www.unige.ch/droit/pi/research/research-colloquium/research-colloquium2019

MORNING SESSION

The first session was chaired by **Prof. Giovanna Di Marzo Serugendo**, University of Geneva.

Dr. Manuel Suter, Coordinator of the Swiss National Cyber Risk Strategy, Reporting and Analysis Centre for Information Assurance MELANI, opened the session by elaborating on the *Swiss Cybersecurity Strategy*, explaining notably how Switzerland is addressing the topic of cybersecurity and what are the specific challenges faced by the federal authorities. He went over the seven strategic objectives of the 2018-2022 National cyber strategy (which is currently in the implementation phase), namely:

1) Switzerland has the skills, knowledge and ability to identify and assess risks, notably by working with researchers and specialists in the field;
2) Switzerland is developing effective preventive measures;
3) Switzerland can manage long-standing and cross-sectoral incidents;
4) Critical infrastructures are resilient to cyber risks and can keep functioning even while under attack;
5) The protection of Switzerland against cyber risks is perceived as a joint task of society, the economy and the state (and not just the government's responsibility), collaboration being essential in this field;
6) Switzerland is committed to international cooperation to enhance cyber security, as it is a phenomenon that needs to be addressed jointly by all nations whenever possible (a task that is not always easy due to political tensions over this topic);
7) Switzerland learns from cyber incidents at home and abroad.

In order to achieve these objectives, the federal authorities have identified ten areas of action and 29 concrete measures within those ten areas. A series of changes have been incorporated in the 2018-2022 National cyber strategy (in comparison with the previous 2012-2017 National cyber strategy) to expand the target groups and also cover SMEs and the population; develop standardization efforts; consider the introduction of an obligation to report cyber incidents; and make cyber defence an integral part of the National cyber strategy. Dr. Suter elaborated on the federal cyber organization (comprised of the three pillars cyber security, cyber defence, and cyber prosecution) as well as on the *Federal Council decree of 30 January 2019 on the Federal Cyber Organisation*, which notably establishes a cyber committee of the Federal Council and a cyber security competence centre within the Federal Department of Finances. Finally, he discussed the details of the national cyber strategy implementation planning (developed together with cantons, businesses and universities), notably indicating that specific measures concerning standardization and awareness raising have already been implemented within different sectors.

Prof. Diego Kuonen, University of Geneva and Statoo Consulting, then discussed *Cybersecurity in the era of Big Data, Machine Learning and Artificial Intelligence*. He first elaborated on the various cybersecurity sources, access and usage issues of Big Data – defined as the accumulation of data that can not be processed or handled using traditional data management processes or tools–, noting that data management is the starting point for any successful data-driven cybersecurity or AI strategy. Data are also at the heart of the "Internet of Things" (IoT) hype, and both Big Data and IoT can be described using the same "five V's", namely: Volume, Variety and Velocity as “essential” characteristics of dataand Veracity and Value as their “qualification of use” characteristics, with Veracity (i.e. “trust in data”) and the related data quality as key. Prof. Kuonen noted that data can be seen as the “fuel” and analytics (i.e. algorithms allowing to learn from or make sense out of data) can be seen as the “engine” of the digital transformation and data-driven cybersecurity; in other words, if nothing is to be done with the data, then there is no use in collecting any. However, data-driven cybersecurity starts with trust, simple because data collected for analytics must be trusted.

Prof. Kuonen then discussed the importance of data with regard to machine learning (ML), which explores the study and construction of algorithms that can learn from and make predictions on (yet-to-be-seen) data, and help make decisions, and with regard to AI, i.e. machines capable of performing tasks normally performed by humans (“learning machines”). He explained that these two technologies are particularly helpful with regard to malware infections, detecting network anomalies, detecting intrusions, rank aggregation and deep packet inspection. However, these technologies are not “inherently” intelligent and need to analyse data to develop their “intelligence”. Therefore, trustworthy data is essential for the results to be relevant and useful, and data should thus be treated as a key strategic asset, so ensuring their veracity and the related quality become imperative.

Prof. Kuonen concluded by noting that all these technologies can help complement and augment humans to strengthen existing cybersecurity setups. Indeed, cybersecurity is not about the technologies, which change too quickly; rather, we should focus on transformation (which can only be accomplished by humans, not hardware), and to make good use of digital opportunities to develop better business strategies.

Discussion then moved to *Liability for AI-based cyberattacks* with **Dr. Omri Rachum-Twaig**, Research Fellow, The Federmann Cyber Security Center, Hebrew University of Jerusalem. Although most people discussing cybersecurity usually focus on cyber-attacks and cyber defence, it is important to remember that cybersecurity implies a secure cyberspace not only against cyber-attacks, but also with regard to how we can expect stakeholders – including AI – to conduct their actions in cyberspace (i.e. standard setting). Although AI has existed for a long time, only recently has it become truly “intelligent” in the sense that it can deal with situations it was not programmed to encounter – and thus “act” on its own. This can lead to some unforeseeable outcomes, as we have seen with the Facebook chatbot case (described by Dr. Benhamou above) and the Tay bot case where a bot launched by Microsoft started tweeting racist remarks that it had never been programmed to make. AI actions can therefore give rise to a series of potential risks and damages – such as physical injury, damage to property, privacy violation, non-monetary damages, denial-of-service of critical services, and damage to autonomy – that need to be considered under tort law.

Some legal frameworks – such as product liability, abnormal dangerous activities, negligence, strict liability and mandatory collective insurance frameworks – applicable to various regulated agents (i.e. manufacturers, distributors, operators and users) can already suggest, in part but not in full, answers to questions of AI liability. However, the main problem remains that liability requires an agent, and robots are not considered legal agents yet (although there has been some talk in the EU to create this agency); as such, they cannot be held responsible under any legal regime. It is therefore necessary to reflect on how we can attribute the act of an autonomous device to a human agent (lines of thought could be found in the vicarious liability and/or principal/agent relationship principles). Another important issue with AI liability relates to foreseeability. Indeed, some AI outcomes cannot be foreseen, understood or explained by humans, and even when some functionality can be logged and traced back, the algorithm cannot necessarily be explained. This hinders the possibility of imposing liability under existing regimes. In fact, all the existing liability regimes identified at the beginning of this paragraph have important shortcomings when it comes to imposing liability on AI/robots. This brought Dr. Rachum-Twaig to conclude that we need to reflect on other tools or avenues – such as oversight and monitoring duties, mandatory backdoors ("emergency brakes" by design), duty of instruction and/or ongoing service and patching duties – if we wish to regulate these issues.

Maria Bicsi, Project Manager, PSYND IT Security Services, was the last speaker of the morning and presented on her firm's *Cybersecurity toolkit for GDPR compliance*. Although the GDPR is a EU regulation, its extraterritorial application to international entities dealing with EU customers is now well-known, and many Swiss entities are therefore concerned. As the GDPR aims to protect personal data and sensitive data, it has a direct impact on cybersecurity, and proper compliance planning can help entities achieve better cybersecurity. PSYND's proposed toolkit contains four main steps: (1) assessment to determine whether the organization is affected by GDPR and to understand the company's maturity level with regard to cybersecurity; (2) design of the required actions to become GDPR compliant; (3) implementation of technical and operational measures and (4) continuous monitoring of the implemented measures and controls. As it has been said earlier in the conference, understanding the data held by a company is paramount to implement adequate compliance measures and controls; indeed, correct and complete data mapping and data classification activities are required to see what kind of measures must be put in place, thus preventing data loss to the best extent possible. Data encryption and pseudonymisation measures are also important, as they lead to less GDPR breaches and smaller penalties in case such breaches occur.

PSYND's Identity & Access Management (IAM) – a security practice ensuring that the right individuals have access to the right resources at the right time – can help businesses comply with the GDPR's general requirements. IAM implementation is generally comprised of three steps: (1) Access Management, which helps minimize unauthorized access to personal data and prevent its disclosure; (2) Identity Governance, which helps ensuring that only the authorized people have access to the resources they need to perform their job and defining segregation of duties and the least privileges; and (3) Privileged Identity Management which enables proper control and monitoring of administrative credential usages. Finally, PSYND can also help companies implement next generation ML-based firewalls to protect all electronic devices, provide various employee trainings in relation to its services, and offer security incident and event management (SIEM) services if needed.

AFTERNOON SESSION

The second session of the day was chaired by **Dr. Yaniv Benhamou**, University of Geneva.

Prof. Rolf H. Weber, University of Zurich, opened the session with a presentation on *Liability for cybersecurity breaches and IoT*. Agreeing with Prof. Kuonen's interpretation of the notion of IoT, he mentioned that the term "things" should be replaced by the more precise term "data". According to Prof. Weber, the cyber threat landscape has multiple facets: threats can come from different agents and/or different tools, and can be of different types, making it difficult to implement a legal framework governing cybersecurity in general. Notwithstanding the difficulties, multiple efforts have been made within the international community to establish a legal framework for cybersecurity, some having more success than others. At the global level, international organizations such as ITU and WTO are based on multilateral treaties touching upon cybersecurity and the UN Group of Governmental Experts (GGE) has issued reports and recommendations on the topic. At the European level, the topic has been addressed by the Council of Europe in the Budapest Convention, and by the EU in the Directive on security of network and information systems (NIS Directive) and the EU Regulation 2019/881 (Cybersecurity Act). At the supra-state level, NATO's Tallinn Manual and East Asia's Shanghai Cooperation Organization are examples of initiatives that have attempted to address the question.

Distinguishing between the various risks posed by IoT and potential solutions is important. A distinction can be made between low and high risks (especially for international organizations such as WTO whose Member States cannot justify trade barriers for low risks). Risks can secondly be addressed either by way of private standards or governmental regulations (however, private standards seem to be preferable as they can evolve more quickly than regulations); either in international or national law; and either in criminal or civil law. As for the main IoT liability challenges, Prof. Weber identifies three major challenges: First, the traditional liability concepts (such as contract, tort and product liability) need to be adapted to these new technologies. For instance, contract law should be modernized to adequately cover "smart contracts", taking into account the risk spheres concept and the cheapest cost avoider concept; product liability law should take into account design problems and information problems related to IoT, and be expanded to cover services (including software) as well as goods (in that regard, the EU Commission is going to present a revised Product Liability Directive soon which will cover software and services, but it is not yet known if Switzerland will follow); and the notion of duty of care under tort liability should be adapted to take IoT issues into account. Second, the accountability concept needs to be developed because IoT causes governance and trust issues, and lawyers will need to develop guidelines in that regard. Third, sector-specific regulations such as telecommunications law and data protection law (i.e. GDPR) need to consider the new IoT reality.

As a solution to these shortcomings, Prof. Weber suggests the design of new legal rules that are adjusted to IoT, including a revised duty of care notion. He also encourages lawmakers, academics and practitioners to reflect on the concept of shared responsibility (risk allocation), to consider implementing new certification frameworks and "half-binding" recommendations (one example of this is the NIST Certification in the U.S.), to create new risk management models and to expand on voluntary or mandatory insurance schemes.

Sotiria Kechagia, Researcher, University of Geneva & C4DT, EPFL and **Dr. Juan Ramon Troncoso-Pastoriza**, Post-doctoral Researcher, EPFL, spoke next on *Liability, Privacy and Security in Medical Data Sharing*. Ms. Kechagia first elaborated on the civil legal liability issues raised by this practice.[3] With more than five declared breaches per week in the U.S., each affecting

[3] The Swiss Penal Code in articles 321 and 321bis defines the penal liability in the event of breach of research data involving human beings.

more than 500 patients each time, and medical/health data alleged to be more precious than other data for hackers, researchers are rightly concerned about the privacy of medical data in today's technological world. Hackers can breach clinical research data at various stages of the process, including those of project submission, analysis and storage of data, and even publication results can be hacked and building a safe environment for the protection of the privacy of patients is an immense concern for researchers.

In Switzerland, many laws directly or indirectly cover the protection of the research data and its further use including (1) the Human Research Act (HRA)[4]; (2) data protection legislation such as the Federal Act on Data Protection (FADP) and the Ordinance concerning the federal law on the protection of data (OLPD); (3) the Swiss Civil Code (art. 28-28I on the protection of personality; (4) the Health Insurance Act; (5) the Therapeutic Products Act; (6) general tort law (art. 41 of the Code of Obligations) and the Product Liability Act of 1994; (7) the Federal Constitution's art. 13 on the protection of privacy; and (8) the GDPR (when it applies to Swiss corporations). Ms. Kechagia identified multiple legal challenges posed by this legislation regarding medical research data sharing, including some pertaining to informed consent (recently the Swiss hospitals adopted a uniform general consent form); the need for a flexible ownership schema of data that passes through multiple persons and entities during the research project and at the same time, respects to the privacy of the patients' sensitive information; the necessity of creating codes of conduct for researchers to address the aforementioned legal gaps; the issue of the management of sensitive Big (Health) Data and esp. the need to increase standards about storage and accessibility of health data; and the fact that genomic data- as the most sensitive health data- is not fully anonymisable (ML techniques can often de-anonymize it). Other issues arise because multiple liability sources and rules need to be connected and analysed together. These include the Federal Act on Data Protection (FADP)-currently under review, the 26 different cantonal legislations on data protection and the Swiss Personalized Health Network (SPHN) initiative (which, for example, in spring 2019 introduced a template data transfer and use agreement (DTUA) regulating inter alia the allocation of liability to be used by the researchers involved in research projects in Switzerland). Further legal constraints are the rules pertaining to disclosure of secondary findings to patients (raising the question of whether the researcher is liable if she/ he does not disclose these findings to the patient). In sum, the applicable law to assess liability for breaches of medical data depends on the type of research and the data involved, and many ethical, legal and technological challenges regarding the regulation of the use of medical research data in the context of precision medicine remain to be addressed by all involved stakeholders together.

Dr. Troncoso-Pastoriza followed by elaborating on the technological aspects of privacy protection in the medical field. He noted that we have seen a plethora of attacks against genomic privacy in the past years, and multiple studies show that standard de-identification and anonymization techniques are ineffective with genomic data. The goal of P4 (Predictive, Preventive, Personalized and Participatory) medicine is to revolutionize healthcare by providing better diagnoses and targeted preventive and therapeutical measures; however, many technical challenges still prevent health professionals to achieve this goal. In order to increase the security of data associated with P4 medicine, Dr. Troncoso-Pastoriza suggested adopting a distributed approach (i.e. to split the

[4] Art. 19 of the HRA will generally cover the liability of the researcher or institution for damage suffered by patients in connection with a project; however, if the data is anonymized, the FADP instead of the HRA will apply.

data between different implicated entities) instead of a centralized approach (where all the data is located in a central repository that can be more easily hacked).

Dr. Troncoso-Pastoriza then explained the different technologies currently available for privacy and security protection – such as traditional encryption, homomorphic encryption, secure multiparty computation, trusted execution environments, differential privacy and distributed ledger technologies (Blockchains) – and their advantages and disadvantages. He also differentiated the various system and threat models, distinguishing between "honest-but-curious" adversaries and "malicious-but-covert" adversaries. He identified two main privacy and security challenges for medical data sharing. The first one is the loss of data confidentiality due to illegitimate access to the data by an external or internal attacker. The second one is patient re-identification due to legitimate access to the data (for instance when malicious users perform "smart" data requests in order to re-identify patients on a specific dataset, such as patients with HIV). He concluded by noting that the confidentiality of health data is in jeopardy worldwide and that the problem is likely to keep increasing since precision medicine dramatically increases the amount of available data. As such, technology alone will not solve the problem and privacy should not be seen as a barrier but rather as an important tool to help prevent it. He ended his presentation by noting that the Data Protection in Personalized Health Project is a direct Swiss response to these concerns.

Gadi Perl, Research Fellow, The Federmann Cyber Security Center, Hebrew University of Jerusalem, moved on to discuss the complex question of whether car manufacturers should be liable for cyberattacks on autonomous vehicles. Autonomous vehicles are cars are made of an aggregation of technologies including sophisticated sensors, AI-based picture recognition and decision tree algorithms, and connectivity, in addition to the mechanical vehicle itself. The question of liability of manufacturers for cyberattacks on those cars has only become recently relevant, now that full control can be passed on to the vehicle, as most accidents before that time were caused by human error. Moreover, the potential solution of imposing liability on the manufacturer could only apply in cases where only manufacturer-made or authorized parts are installed in the vehicle (since it is much more complicate to allocate liability when third-party applications or parts are installed)

Currently, most regulatory systems still focus on the liability of the driver and cannot apply to accidents "caused" by automatic vehicles. Mr. Perl predicts that people inside the vehicle could eventually be seen as passengers or "cargo", and autonomous vehicles could be seen as a service like a taxi or Uber. According to him, one main element to consider when trying to establish a new liability regime is the vehicle's connectivity, e.g. its ability to connect with other vehicles and infrastructures, and data surrounding it. Connectivity has advantages in that it allows the vehicle to make informed decisions in advance and assists in accident prevention. However, the vehicle is also hackable from the moment it is connected, creating a load of criminal, national security and data privacy issues.

The already existing doctrines of negligence, product liability and strict liability can suggest some lines of thought to hold manufacturers liable in case of an accident caused by an autonomous vehicle, but too many gaps and questions remain to conclude that these doctrines bring satisfactory solutions. Mr. Perl indicated that there are pros and cons to holding manufacturers liable in case of such accidents. On the one hand, this would be a cost-effective solution, since manufacturers have the most knowledge on the vehicle and are best suited to fix any issues that may arise. It is also simple to implement and takes into account the fact that there is no driver in an autonomous vehicle.

On the other hand, however, it does not seem logical to impose liability on manufacturers when they do not control the vehicle or its use. In addition, such a liability regime may create barriers to competition and harm private interests such as property and privacy (for instance if manufacturers start forcing updates on the vehicles by the owners, in order to protect themselves). Mr. Perl's proposed solution is to establish duties, notably by formalizing safety standards, regulating licenses, and creating safe-harbours (allowing manufacturers or other stakeholders to be safe from prosecution if they follow a series of preventive steps). Mr. Perl predicts that the increase in autonomous vehicles on the roads worldwide will radically change the manufacturer/end user relations. Indeed, we will need to reflect on potential obligations regarding updates to the vehicle's software. These kinds of update obligations will oppose security (for the manufacturer) and property (for the owner) rights, will require the creation and application of standards determining when an update becomes urgent, and may pose additional issues when the update requires new hardware (i.e. who is responsible to pay for it?). It will also be important to consider both post-fact enforcement measures but also preventive measures if we want a functional liability regime.

Luigi Bruno, Senior Consultant in Cyber Risk, Deloitte, moved on to discuss *"State of the Art" in IT security* that organizations are required to implement. He first noted that the relationship between "State of the Art" and law seems unclear, because law stays silent on what these technical and organizational measures really are. The two most widely recognized European regulations on cybersecurity and data protection are GDPR and the NIS Directive. The similarities between these two regulations are that they both mention "the State of the Art" and both focus on technical and organizational measures (GDPR Article 32 and NIS Article 14). This raises the question what "State of the Art" really is.

The definition of "State of the Art" and IT security becomes clearer inside organizations, who usually implement both technical and organizational/legal measures with regard to IT security. Most often technical security measures include VPN, encryption, network segmentation, remote access, cloud storage and web security. Problems implementing technical measures may arise from the fact that implementation can be very expensive, and that technical and legal sides of the organization might have different knowledge and might not understand each other. At the same time, organizations usually also implement organizational and legal measures, which include for example protection and access policies, risk management frameworks, governance structure, compliance and legal structure etc. Mr. Bruno pointed out that too much focus is often put on implementing technical measures, when the most important part is the implementation of organizational measures. Mr. Bruno took as an example a real case where a cyberattack hit a large shipping factory who started to lose important amounts of money, but no one knew how to proceed to stop it. Eventually, the company started to build their own IT infrastructure and hired consultants around the world.

But how to make sure that organization know what to do when they face a cyberattack? According to Mr. Bruno, they need to simulate cyberattacks beforehand, and a number of organizations have already started doing this. The company needs to be guided through the whole simulation, so that everyone knows what do to if a real attack happens. The key is to prepare stakeholders and departments to leverage implemented measures to jointly resolve and report incidents in a compliant way. Communication and coordination between Data Protection Officers, Chief Information Security Officers, Legal Counsels, Compliance Officers, and C-Suite stakeholders is of utmost importance. Knowing what to do in a cross-functional collaborative manner is the true "State of the Art".

Justine Ferland, Research and teaching assistant, University of Geneva, closed the afternoon session by discussing *Insurance coverage for cyberattacks: lessons from the Mondelez v. Zurich case*. Insurance questions are important to cybersecurity because cybercrimes can lead to extremely high damages; yet, there are still a number of important issues that need to be addressed before the cyber insurance market can really increase cyber protection for policyholders. One of these issues is whether war exclusions found in most insurance policies apply to state-sponsored cyberattacks, and if yes, under what conditions. This question is in the heart of *Mondelez v. Zurich (Insurance Group)*[5] case that is currently pending. In this case, Mondelez's networks were attacked by the NotPetya virus which caused important damages. At the time of the attack Mondelez held an all-risk property insurance policy from Zurich. Zurich refused to pay according to a policy exclusion for damage resulting from a hostile or warlike action by a government or a sovereign power, claiming that Russia was behind the attack, which led Mondelez to sue Zurich for breach of contract.

Ms. Ferland identified two key issues in the case. The first one is the attribution of the cyberattack by Zurich to a government or a sovereign power, in occurrence Russia, which will not be easy since Russia's involvement in the attack was never officially proven. The second key issue is the interpretation of the war exclusion in a cyber context. According to the policy, the attack has to be "hostile or warlike" for the exclusion to apply, and it is unclear whether this wording can be interpreted to cover state-sponsored cyberattacks. Since the wording of the policy exclusion does not clearly apply to the NotPetya attack, the court in this case will likely adopt a narrow interpretation of the exclusion (in line with earlier case law) in favour of Mondelez. Ms. Ferland therefore believes that this will be a difficult case for Zurich.

The Mondelez case is a purely contractual insurance dispute between two American companies and it is unlikely that the Court will feel the need to deviate from U.S. insurance law in its judgment. However, the questions raised by the case are universal, and all insurance companies should reflect on them if they want to adjust to the new reality of cyberattacks. In that light, Ms. Ferland suggested three other useful legal frameworks to examine the applicability of war exclusion clauses in insurance contracts in the context of state-attributed cyberattacks. The first relevant legal framework is general contract law and especially the force majeure exemption. Although the exclusion clause in the Zurich policy is not technically a force majeure clause, there are many similarities between the two types of clauses the principles developed under the force majeure doctrine could still serve as inspiration. A second relevant legal framework is the international law of armed conflict doctrine. It is clear that cyberattacks can now be qualified as acts of war (under certain conditions) in international law; yet, not every cyberattack reaches the threshold of being considered as a warlike action. A third relevant legal framework could be found in the principles supporting Microsoft's proposal for a "Digital Geneva Convention".

The Mondelez case will have an important impact on the limits of insurance policies with regard to damages caused by cyberattacks. Until a judgment is rendered, both companies and insurers

[5] *Mondelez Intl. Inc. v. Zurich Am. Ins. Co.*, No. 2018-L-11008, 2018 WL 4941760 (Ill. Cir. Ct., Cook Cty., complaint filed Oct. 10, 2018)

should reflect on the contents of their present and future insurance policies. Businesses may wish to seek specific cyber coverage, even when their regular all-risk policy seems to be applicable. Insurance companies should make sure that their war exclusion clauses do not leave room for interpretation. Finally all businesses including insurance companies themselves should ensure to have strong cybersecurity measures and comprehensive cyber risk management policies in place to limit exposure in the first place.

Justine FERLAND, Cyber insurance – What coverage in case of an alleged act of War? Questions raised by the Mondelez v. Zurich case, Computer Law & Security Review, Volume 35, Issue 4, August 2019, Pages 369-376. Available online at: https://doi.org/10.1016/j.clsr.2019.06.003

Justine Ferland and Helen Happonen, University of Geneva, July 11, 2019