www.cybersecurity-liability.ch

WHAT CIVIL LIABILITY FOR CYBERATTACKS?

CONFERENCE REPORT

INTRODUCTION

On June 21, 2018, over 130 participants attended the Geneva Cybersecurity Law & Policy Conference: What Civil Liability for Cyberattacks?, held in the framework of a research project between the University of Geneva and the Hebrew University of Jerusalem. This conference aimed at presenting selected legal and policy aspects of cybersecurity in a crosscutting approach. It was co-organized by **Prof. and Vice-rector Jacques de Werra** and **Dr. Yaniv Benhamou** from the Faculty of Law of the University of Geneva, as well as **Prof. Guy Pessach** and **Dr. Tamar Berenblum** from the Cyber Security Research Center of the Hebrew University of Jerusalem.

The conference opened with some introductory remarks from **Prof. Yves Flückiger**, Rector of the University of Geneva, who noted that Geneva is one of the capitals of cybersecurity and digital technology, thus making it the perfect place to hold the conference. In addition, the canton had just published, a day prior to the conference, its new policy on digital economy which includes provisions on cybersecurity. He stressed the importance of investing in teaching and research on this fast-changing topic and of creating a discussion platform allowing technical experts and policymakers to work together.

Prof. Bénédict Foëx, Dean of the Faculty of Law of the University of Geneva, indicated that this conference was significant for three reasons. First, because of its topic: the interaction

between cybersecurity and policy is highly relevant in today's world, and numerous unresolved issues are at stake. Second, because of the expertise of its organizers, the University of Geneva and the Hebrew University of Jerusalem (the latter boasting a Cyber Security Research Center), who have undertaken a large joint research project examining the legal involvement needed to properly regulate cybersecurity breaches. Third, because it addresses urgent questions that are currently not fully explored nor grasped by lawyers. 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".

Prof. Jacques de Werra, Vice-rector of the University of Geneva, closed the introduction by adding that two partners, the Geneva Internet Platform (GIP) and Clusis, supported the event, which was also part of the 5th edition of the UNIGE Internet L@w Summer School.[1] He 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 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. Moreover, we need to define the nature of this liability: is it criminal, civil, or both? What damages can be claimed? What is the standard of care? What is the role of data protection? How can insurance apply? How do new technologies, such as artificial intelligence (AI), impact the liability of legal persons? The University of Geneva's and Hebrew University of Jerusalem's joint research project hopes to analyze those issues and open certain policy options.

FIRST PANEL
CIVIL LIABILITY FOR CYBER-ATTACKS: SELECTED ISSUES AND CHALLENGES

The first panel was chaired by **Prof. Christopher Bavitz**, Clinical Professor of Law at Harvard Law School (HLS) and Managing Director of HLS's Cyberlaw Clinic, and focused on issues raised by the application of traditional civil liability principles in the context of cyberattacks.

Prof. Guy Pessach, Cyber Security Research Center, Hebrew University of Jerusalem, first mapped the challenges posed by the interaction of cybersecurity, damages and private law. As the world becomes more connected by the minute and as a growing number of business activities involve data, the scale, scope, outreach, intensity and implication of cybersecurity breaches keep increasing. The legal community must reflect on the implications of such changes. Notably, it must determine whether new legal principles are needed to adequately govern cyberspace or if the existing ones are sufficient. Prof. Pessach identified multiple complications that arise when one tries to apply general civil liability principles to cyber harm. For instance, when AI (a machine) causes damages, traditional private law does not explain how to evaluate the liability and duty of care applicable to legal persons who may not have prevented such damages. It is also unclear how different branches of law, such as criminal and private law, interact together in these situations. Because the causes and consequences of cyber harm may vary greatly from one industry to another, a general legal

[1] https://www.unige.ch/droit/pi/summer-schools/internet-law/internet-law-summer-school-2018

analysis is not sufficient to answer those questions; a bottom-up, industry-based analysis is also concurrently required. Prof. Pessach also addressed two fundamental issues that cybersecurity breaches pose to general liability law. The first one regards *software liability*, e.g. liability for harm caused by software malfunction. Traditionally, software has been regarded by law as a service, not a product; as such, in cases of software failure, one could allege the liability of the developer for negligence. However, Courts have also concluded to strict product liability where software-embedded elements installed in so-called "intelligent objects" have caused harm. Against that backdrop, we must reflect on whether such a distinction between the liability of "naked" software and the liability of object-embedded software is necessary, and whether we need to develop a new legal liability regime that would specifically cover software failures. The second issue pertains to *data protection*. Currently, in most jurisdictions, data protection laws are the main mechanisms aimed at preventing and overcoming cybersecurity breaches. However, these laws may not be sufficient anymore, and we may be overseeing important considerations by focusing so much on data protection; we likely need additional layers of liability to fully cover the question of civil liability for cyberattacks.

Prof. Damian K. Graf, Kalaidos Law School & University of Zurich, examined the interactions between civil and criminal liability for cybercrimes under Swiss law. He based his presentation on a hypothetic example where a hacker gets into a hospital's computer system due to failure from the hospital directors to put a cybersecurity protocol in place, and blocks access to the medical files until a ransom is paid. The directors eventually pay the ransom (pecuniary damage) but meanwhile, some patients die due to the impossibility for doctors to access their medical files (personal injury). In such a case, we may find legal basis for both criminal and civil prosecution of some of the parties involved, most obviously the hacker and the hospital directors. Although the criminal and civil actions would be distinct, each having different defendants and purposes (e.g. punishment under the criminal suit and monetary compensation for damages under the civil suit), some material and procedural interactions would necessarily arise between the two proceedings. Looking at the material interactions between criminal and civil proceedings for hospital directors' liability, for instance, we note that some of the constituent elements of the criminal infraction of mismanagement (art. 158 of the Swiss Penal Code)[2] overlap with the constituent elements of directors' civil liability (art. 754 Swiss Code of Obligation)[3]. In addition, criminal law is often dependent on civil law perspective and vice versa. For example, criminal judges often interpret normative constituent elements of a crime by explicitly or implicitly referring to civil law, a practice that has been endorsed by the Swiss Federal Tribunal. Moreover, in many legal traditions, it has been established that a specific term must be interpreted the same way in any field of law, in order to preserve the uniformity of the legal system. On the procedural side, although rules are obviously stricter under criminal proceedings (protection against self-incrimination, higher standard of proof, etc.), we nonetheless identify some interactions. For instance, it is possible in Switzerland to file a civil suit within criminal proceedings, which allows a civil party to rely on the facts established by the prosecutor and benefit from the evidence

[2] Namely (i) management of assets, (ii) breach of duty, (iii) damage, (iv) causal link and (v) intent.
[3] Namely (i) director status, (ii) breach of duty, (iii) damage, (iv) causal link and (v) fault.

collected by law officers. The criminal verdict also often has a binding effect on civil judges confronted with the same problems (although this is not a legal principle).

Discussion then moved on to insurance protection against cyberattacks. According to **Navid Kimia,** Head of Specialties Romandie, Zurich Assurance, increasing digitalisation highlights various risks associated with the use of new technologies such as the Cloud, interconnected devices (IoT) and intelligent cities, as well as with the ever-growing amount of confidential data stored on various supports. With cybercrime costing over $500 billion yearly to the global economy, managing cyber risk has become a top priority for businesses and governments alike and many now turn towards insurance companies to seek coverage against the consequences of potential cyberattacks – especially now that the General Data Protection Regulation (GDPR) has entered into force. Insurance policies currently cover three types of losses. First, insurance may cover the cost of a business' civil liability, e.g. its defense and indemnification costs if found liable (by negligence, for instance) in the context of a cyberattack that has caused harm to third parties. Second, insurance may cover the business' breach costs, e.g. the direct economic consequences of the attack such as complying with regulations following the breach, notifying customers, obtaining legal counsel, detecting/quantifying/recovering from incident, and managing public relations. Third, insurance may cover the costs related to business interruption (loss of revenue) following a breach. However, an increasing number of companies are also seeking coverage against potential product liability, especially regarding physical harm (for instance following the hacking of autonomous cars). Although well aware of this issue, the insurance industry is not yet able to properly evaluate the risk, and thus product liability is currently excluded from all insurance policies.

Prof. Stacey L. Dogan, Cybersecurity Alliance, Boston University, addressed trends and perspectives regarding cybersecurity liability in the United States. She explained that although the American legal landscape is not as structured as the European GDPR, it is nonetheless well furnished by a complex set of interrelated standards found in federal law, State law and private obligations. On the federal level, the FTC Act, which is the main statute governing consumer protection against unfair or deceptive trade practices throughout the United States, applies in the context of major security breaches. So far, however, Courts have only rendered a few final decisions concerning the data protection obligations of private actors. Legal actions have mostly resulted in consent decrees, e.g., in cybersecurity matters, public settlement agreements in which a party undertakes to implement certain measures without admitting its liability. These consent decrees have created a sort of "privacy common law" establishing best practices regarding consumer data protection. In addition, some sector-specific federal statutes and regulations also govern data-intensive or sensitive industries such as the health, education, finance and telecommunication sectors. On the State level, data breach notification laws coexist with acts governing unfair and deceptive acts and practices (UDAPs), under which State attorneys general may prosecute wrongdoers – often more aggressively than their federal counterparts. Settlements in those cases may result in voluntary compliance agreements, the State-equivalent of consent decrees, defining best practices for future actors. The States of Massachusetts and California have also enacted specific data security statutes and provided formal guidance to strengthen consumer

protection against data breaches.[4] Finally, various private ordering trends such as best practices (emerging from consent decrees and voluntary compliance agreements), voluntary frameworks and standards (e.g. NIST and CIST Controls), certifications authorities (e.g. CISSP) and licensure bodies, and a growing "privacy bar" complete this legal panorama. Prof. Dogan also exposed two issues that are currently unresolved in privacy breach actions. First, the question of standing to sue is still unclear due to the *Spokeo Inc. v. Robins* case, in which the Court has confirmed that a concrete injury is required for standing; in other words, alleging a mere violation of the law without actual damages is not sufficient. Although it has been clarified that disclosure of financial information to third parties constitute a tangible injury, there is still uncertainty as to other types of injury that may or may not be concrete enough in cybersecurity breach matters (e.g. emotional distress as the result of disclosure of private information). Second, the notion of "substantial harm" required for a FTC action has not yet been defined, thus uncertainty lingers; however, States have more flexibility in this regard and may analyze "harm" in a more generous way. Prof. Dogan concluded her presentation by noting that in the actual political context, developments in the law of cybersecurity and data protection will likely come from the States, not the federal government.

The last speaker of this first panel, **Dr. Michael Kende**, Senior Advisor, Analysis Mason & Visiting Professor, Graduate Institute of International and Development Studies, discussed the economics of cybersecurity. Studies have shown that 93% of cyberattacks are linked to known vulnerabilities or social engineering, and are thus preventable. The consequences of the remaining 7% of (unpreventable) cyberattacks could still be mitigated if businesses were to retain less data and encrypt what is kept. Reiterating that cyberattacks cost over $500 billion yearly to the global economy, all while causing loss of customers, jobs and privacy, Dr. Kende questioned why isn't our society doing more to prevent or mitigate them. He noted that early inaction in such cases is rather common, giving the example of seat belt use and air bag adoption in vehicles, which took decades to be legally and commonly implemented due to economic challenges despite clear reports and public awareness campaigns on their importance. Today, we are seeing a similar situation with, notably, the use of password managers to increase password security. Even though password managers are crucial for cybersecurity, they are currently evaluated on the market based on various features that do not touch upon safety. Dr. Kende also identified two main cybersecurity market failures. First, he noted that the current cybersecurity framework creates *negative* externalities – e.g. negative financial consequences affecting third parties instead of the concerned party. In the Target data breach that impacted 40 million shoppers whose credit card information was stolen, for instance, losses were estimated at over US $200 million, yet Target was only ultimately compelled to pay for replacing the hacked credit cards. Because organisations do not bear all the costs of a data breach – e.g. there is little internalisation of costs –, they are less inclined to invest in preventing future breaches, on the basis that it is not economically profitable (prevention would cost more than potential liability). Second, there is a lot of

[4] See for instance the *Commonwealth of Massachusetts v. Equifax* (April 3, 2018) case: "The Attorney General, unlike a private litigant (…) is required only to prove that unfair or deceptive acts or practices took place in trade or commerce; she is not required to prove or quantify resulting economic injury. (…) She is not required to allege or prove that any individual consumer was actually harmed (…)".

asymmetric information in the current cybersecurity framework – meaning that one party to an economic transaction is more knowledgeable than the other. Because customers usually do not possess the technical or legal expertise to assess the cybersecurity level of businesses they are dealing with, the latter are less inclined to invest in cybersecurity measures. Dr. Kende explained that these market failures require external solutions. He suggested implementing technology designed around human behaviour (e.g. automatic security updates on operating systems and default password managers). Legislators could also draft regulations to address the market failures. For instance, negative externalities could be eliminated if legislation internalised breach costs and increased breach liability through mandatory disclosure or stronger consumer protection laws, while asymmetric information could be countered by regulating features that consumers cannot verify or assess (e.g. requiring encryption of stored data). Non-regulatory solutions such as security testing/ratings and certification that sets basic standards for cybersecurity could also be envisioned. Dr. Kende concluded by reminding that new technologies such as intelligent devices raise additional allocation of liability issues which inevitably have an economical impact, and illustrated this with a recent example of a failure in the Internet-enabled entertainment system in Jeep Chryslers that allowed remote hacking.

SECOND PANEL
DATA PROTECTION AND CUYBERSECURITY BREACHES: WHAT RISKS OF LIABILITY?

The second panel, also moderated by **Prof. Bavitz**, explored risks of liability due to data protection and cybersecurity breaches from various national and regional legal perspectives.

Dr. David Vasella, Attorney at law, Walder Wyss and Lecturer, University of Zurich, first explored the question under Swiss law. He noted that the Swiss Data Protection Act (DPA) – which is currently being revised in line with the GDPR, but should not change much with regard to the concept of liability – and the Data Protection Ordinance (DPO) of 1993 impose a generic obligation on controllers and processors to take appropriate security measures against data breaches.[5] Specific obligations also apply in the financial sector; for instance, the *FINMA Circular on operational risks* stipulates that banks must implement an IT risk management concept, notably for dealing with cyber risk. Those who violate those obligations may incur civil liability. The general definition of "civil liability" under article 28a of the Swiss Civil Code requires either a contractual breach (e.g. breach of a data processing agreement) or a tort (e.g. breach of data protection law) with proof of fault, damage and causal link in each case. The fault can be any wilful or negligent action or omission by any party (controller, processor, member of the board, etc.). Damages under Swiss law are generally limited to economic losses[6]; this means that embarrassment following a breach and immaterial damages are not covered and damages for pain and suffering are rarely granted.

[5] A "data breach" may be defined as any unauthorized processing of data, including a breach of a processing principle.

[6] The Swiss Federal Court has defined a damage as "the involuntary reduction of net assets; it corresponds to the difference between the current amount of the injured party's assets and the amount that the same assets would have if the harmful event had not occurred" (133 III 462, 4.4.2).

Commenting on the role of the GDPR in Swiss law, Dr. Vasella reminded that while the GDPR does not directly apply in Switzerland, it does apply to Swiss businesses who are either offering goods and services in EU countries, monitoring the behaviour of EU residents or dealing with residents of the EU/EEA. As such, Swiss companies may have exposure if they do not fully implement the GDPR. Dr. Vasella further discussed the web of available legal claims in case of a data breach affecting a data processor. Multiple parties may have claims based on contract and/or tort towards the controller and/or the processor jointly and severally[7] (the controller being liable for the processor under the GDPR and Swiss law). For instance, data subjects may claim damages (including non-material damages if they are in the EEA) against both the controller and processor based on tort; the controller's contractual partners may claim damages against the controller (based on contract and potentially tort) and processor (based on tort); authorities may investigate and potentially fine both controller and processor; and the processor itself may have a claim against the controller based on contract and/or tort. However, because the implicated parties generally limit their liability or allocate risks differently through contracts[8], not all those claims may be pursued in all situations and a careful analysis is necessary in every case.

Limor Shmerling Magazanik, Director of Strategic Alliances at the Israeli Privacy Protection Authority (IPPA), followed by discussing liability risks from an Israeli perspective. She explained that the data protection system put in place in Israel resembles that of the EU and that the IPPA has vast enforcement powers over both public and private sector organizations. In Israel, privacy protection within the digital sphere is seen as a way to protect basic human rights and multiple legal sources are applicable in that regard. First, some obligations are found in the Basic Law pertaining to human dignity and liberty. A specific Protection of Privacy (PoP) Law also poses the general principle that processors and controllers are responsible for data security. PoP Regulations provide further details on this obligation. A PoP Regulation on Data Security, which governs the entire country, notably ensures that every data controller in Israel implements specific cybersecurity principles in their routine operations. Its goal is to create normative clarity and establish a unified minimum standard of cybersecurity to avoid situations where data controllers claim to respect cybersecurity principles without having implemented anything specific. It also has international applicability and implements a modular approach based on four levels of risk. PoP Regulations on Trans Border Data Flows, PPA Guidelines and Supreme Court rulings complete the legal panorama of cybersecurity in Israel. Ms. Shmerling Magazanik further explained that organizations are required to follow three steps to comply with Israeli privacy legislation: (1) prepare a data mapping and risk analysis, (2) set appropriate security procedures to protect this data, and (3) implement security measures. Serious breaches must be immediately notified to the IPPA, who *may* order public notification if necessary or relevant. Timely breach notification is encouraged by a "first year enforcement policy"; this means that businesses who duly declare data breaches to the IPPA will benefit from softer enforcement measures (for instance, the investigation will generally not be published) than businesses who do not. It is also interesting to note that Israeli data protection law allows class actions and does not require proof of damages under a certain amount. Ms. Shmerling

[7] Articles 50 et seq. and 99(3) CO.
[8] Although both the GDPR and Swiss law forbid limitation of liability in specific cases.

Magazanik concluded by reminding the audience that effective data protection policies may only be achieved through the combination of good legislation, good enforcement procedures and good technological knowledge.

The audience then traveled back to Europe with **Olivier Matter**, European Data Protection Supervisor, who presented the cybersecurity liability framework from EU/GDPR perspectives. With the GDPR having just entered into force on May 25, 2018, data protection in Europe has moved from an ex-ante approach to an ex-post approach. Although the GDPR does not revolutionize data protection principles, it does reinforce them and confer more power to data protection authorities. Under the GDPR, businesses must notify a personal data breach[9] to the supervisory authority (art. 33) and communicate the breach to the data subject (art. 34), subject to possible restrictions found in Recitals 85 to 88. The *Guidelines on Personal Data Breach notification under GDPR* of the Article 29 Working Party provide further guidance to that effect. The GDPR then imposes different duties on data controllers depending on the degree of risk associated with the breach. First, in every situation (even in the absence of risk), controllers must ensure accountability and data security by following an incident management procedure. In addition, if the breach is likely to result in a risk to the data subject (based on factors such as the nature of the breach, the categories of data, the number of data subjects concerned, whether a DPO or other contact point is involved, and the potential consequences to mitigate), said breach must be notified to the competent supervisory authority without undue delay (e.g. not later than 72h after the controller becomes aware of the breach). The processor must also notify the controller of the breach and assist it with all necessary means. Alternatively, if the personal data breach is likely to result in a high risk to the data subjects, these data subjects must be notified of the breach as soon as possible. Recitals 75 and 76 of the GDPR provide guidance on assessment of risks (to determine whether a breach is likely to result in a risk or a high risk to the data subject). They notably establish that the assessment must consider the potential severity of the breach and likelihood of impact on the rights and freedoms of data subjects. The nature, sensitivity and volume of data involved also play a role, especially when special categories of individuals (such as children or other vulnerable individuals) or data controllers (such as hospitals) are concerned. In that regard, Mr. Matter proposed a matrix that could be followed. Finally, Mr. Matter noted that the GDPR has also heightened sanctions and remedies that may be imposed by data protection authorities, the whole to hopefully mitigate data breaches and their impacts in the EU.

THIRD PANEL
RISK MANAGEMENT: WHAT STANDARD OF CARE FOR VICTIMS OF CYBER-ATTACKS?

The third panel analyzed the standard of care applicable to potential victims of cyberattacks and was chaired by **Dr. Yaniv Benhamou**, Lecturer, University of Geneva and Attorney at law, Lenz & Staehelin.

[9] A personal data breach is defined as "a breach of security leading to the accidental unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed" (art. 4(12) GDPR) or an information security breach leading to the compromise of confidentiality, availability and/or integrity of personal data under the responsibility of the controller.

Dr. Michel Jaccard, Attorney at law, id est avocats, first discussed the legal framework and challenges associated with businesses' risk mitigation and management strategies. He indicated that risk mitigation in the context of cyber incidents is a complex task: on the one hand, businesses must try to prevent cyber attacks through careful analysis, comprehensive anticipation and detailed planning, yet on the other hand, once an incident occurs, it becomes necessary to act quickly without all the facts at hand. This proves difficult for lawyers who are used to thoroughly investigating relevant facts before taking action. Constructing a legal framework pertaining to cyber incidents is also arduous, notably because the definition of a "cyber incident" in itself is not clear; each industry currently has its own definition in its company policies. For instance, can failure by an employee to renew his password every 3 months (in contravention to company policy) be qualified as a "cyber incident", even if there is no consequence? Does the definition only include successful attacks, or also failed attempts? Does it cover mere risks without exploitation of data, or is actual damage necessary? Understanding cyber incidents is not an easier task; for each occurrence, one must determine the cause (e.g. technological weakness, organizational failure, human negligence), the identity of the attackers, their motivations, and the impacts on the business (e.g. loss of trust, valuable assets or even entire business critical functions). Dr. Jaccard also submitted that the current legal liability framework is not yet adapted to the cyber world. As such, many uncertainties remain and must be addressed by lawyers and in-house counsels. For instance, it is unclear how to enforce a sanction under criminal law; how to recover damages under civil law; how to assign blame under labour law (when employees may be involved); how a business may minimize its exposure towards clients under contractual law; and what industry-specific obligations must be taken into consideration when assessing liability. Moreover, depending on the nature of the cyberattack at issue, different types of reactions may be appropriate; some situations require instant legal engagement while others may simply need internal monitoring. Dr. Jaccard specified that the most important for businesses in every situation, however, is to ensure that appropriate technological and organisational risk mitigation measures are in place, and that policies (such as staff regulations, access control policies and incident response plans) are enacted, internally communicated and enforced. Other appropriate risk mitigation actions include training of personnel, drafting of policies and templates and testing/updating. In light of the above, Dr. Jaccard concluded by suggesting that businesses follow these steps in case of a cyberattack: (1) document the attack, preserve the evidence; (2) assess scenarios and related legal steps; (3) prepare notifications; (4) file criminal and civil complaints; (5) review all internal and external communications; (6) review all business agreements for *force majeure*, business continuity, confidentiality and liability issues.

The next presentations focused on cyber risk mitigation in specific industries. First, **Kim-Andrée Potvin**, Chief Operating Officer, Landolt & Cie, discussed risk mitigation standards in the banking and financial industry. She noted that the open banking infrastructure now required by clients (implying mobility, instantaneity and personalization) is not fully compatible with a bank's data security duties, which notably include ensuring that a client's identity, data and operations are fully protected. Indeed, developing the latter necessarily implies weakening the latter and vice-versa. A "zero risk" approach is not conceivable anymore and the banking industry's objective is therefore to reduce risks as much as possible

while balancing those two elements. However, the balance is currently asymmetrical, because even if a bank blocks 99% of cyberattacks, a sole breach may be fatal to its operations. Ms. Potvin further explained that in the past years, banks have moved from a very secured but very closed "fortress model" to a more open but less secure "airport hub" model. She noted that threats faced by the banking and finance industry are both external (the most common including phishing, hacking and data breaches) and internal (e.g. employees who may, often involuntarily, pose actions detrimental to cybersecurity); it is therefore necessary for these industries to develop a comprehensive data leakage prevention program. In conclusion, Ms. Potvin argued that cybersecurity must be at the core of a company's transformation and development. Indeed, today's innovative banking methods necessarily imply the handling and online transfer of client data, which poses greater risks with regard to data protection; cybersecurity experts must therefore be involved from the start and give their input on all aspects of banking development instead of only being called to solve problems after they have arisen. The finance industry should keep in mind that cybersecurity is an asset: it reassures managers, board members and clients, and provides a strong base on which to build innovative solutions, allowing a business to keep moving forward.

Gadi Perl, Cyber Security Research Center, Hebrew University of Jerusalem, moved on to discuss the complexities of regulating autonomous cars. Concretely speaking, these cars are comprised of an aggregation of technologies including sophisticated sensors, AI-based picture recognition and decision tree algorithms, and connectivity. Mr. Perl argued that the current regulations pertaining to those cars are insufficient. Indeed, recent accidents, such as the accident of a self-driving Uber test car in Arizona in March 2018, have revealed gaps in the current regulatory regime, namely because the liability and privacy legal principles applicable to such accidents are unclear. We need regulation so that people will trust and accept this new technology, which has tremendous societal value (one may think about the lives saved and accidents avoided, the infrastructure improvements, and the social equality brought by the fact that anyone would be able to drive despite their personal health conditions). Although many academics have studied the issue from different points of view (privacy, cybersecurity, liability, ethics, etc.), so far, their theories have been conflicting and none has been able to propose a complete regulation scheme or a holistic solution that is fully applicable to current technologies. Mr. Perl's proposed solution is to regulate autonomous cars by regulating the technologies that compose them. This could be done by dividing the end product into its constructing technologies, namely the sensors, the driving algorithms, the connectivity devices and the mechanical vehicle itself, and defining each of these components up to the level required for regulation. This process would allow us to identify the legal issues pertaining to each component (for instance, the sensors raise privacy and cybersecurity issues, whereas the algorithms raise liability, ethics and risk management questions) and propose adequate regulation to solve them.

Jean Yves Art, Senior Director, Strategic Partnerships, Microsoft, concluded this panel discussion by addressing the standards in the software industry and the role of the Digital Geneva Convention. He explained that two unprecedented ransomware cyberattacks – WannaCry and NotPeyta – have been launched or sponsored by countries against citizens in the last years. These attacks, whose scopes went beyond the more "traditional" cyber crimes such as phishing or hacking, shed light on the dangers associated with the increasing

implementation of artificial intelligence and computing devices in all aspects of our lives, and on the necessity for the international community to take action as quickly as possible. Although a few provisions of international law could perhaps apply to these cyberattacks launched by States against citizens – the prohibition of the use of force in international relations, for instance, could possibly be interpreted as including "cyber force", and it could be argued that such attacks constitute "armed conflicts" under the Geneva Conventions – many gaps remain since international legislation was not drafted with the cyber world in mind. It is against that backdrop that Microsoft introduced the idea of a Digital Geneva Convention to fill in those gaps. Through this Convention, nation States would pledge to refrain from launching cyber attacks at civilians and infrastructures in times of peace. Companies in the tech sector have already taken important steps to limit such cyber attacks and mitigate their effects. In particular, they have recently adopted the Cybersecurity Tech Accord in which businesses pledge to protect consumers worldwide and to refrain from aiding governments to carry out cyber attacks. To date, approximately 50 tech companies have adhered to the Tech Accord.

FOURTH PANEL (DISCUSSION)
THE FUTURE OF CYBERSECURITY: ARTIFICIAL INTELLIGENCE AND OTHER CHALLENGES

Dr. Jovan Kurbalija, Geneva Internet Platform, moderated the last panel of the conference, during which **Dr. Tamar Berenblum**, Cyber Security Research Center, Hebrew University of Jerusalem, **Prof. Solange Ghernaouti**, University of Lausanne, **Marco Obiso**, Head ICT Applications and Cybersecurity Division, International Telecommunications Union, **Prof. Dimitri Konstantas**, University of Geneva and **Christophe Nicolas**, Group Chief Information Officer, Kudelski Group and SVP & Founder, Kudelski Security, discussed about "The Future of Cybersecurity: Artificial Intelligence and other Challenges".

The panellists noted that artificial intelligence (AI) is a very complex concept which poses a plethora of challenges to individual and collective security. One of these problems is that cybercrime is currently studied in different ways by different industries; for instance, computer experts concentrate on the technology used whereas social scientists attempt to find anthropological explanations for cybercrime, but they do not necessarily take the time to reconcile their views and findings. In addition, policymakers usually do not take enough time to engage with those possessing expertise on this technology, in order to understand it better and regulate it accordingly. Top managers are also often oblivious to the cyber dangers looming over their businesses, because the security experts do not necessarily share information with them. We do not know yet whether and/or how AI can be helpful in managing cybersecurity risks (by helping deter attacks for instance) at both State and private levels, so collaboration between different actors is of the utmost importance to find answers.

Another of the challenges making it difficult to adequately regulate data use and cybersecurity is the generation gap. Technology changes so quickly that even if we regulate it today, the next generation will deal with it differently, and the definition of fundamental notions such as privacy will evolve. It is still important, however, to try to build something to

transfer to the next generations, and to keep them in mind when trying to regulate our data use.

We must also remain wary of the dangers of abuse and exploitation of our personal data. It was submitted that the right to be disconnected and the right to know if you are dealing with AI (as opposed to a human being) should be treated as human rights on the basis that cybersecurity must not only protect the cyber world but also, first and foremost, human beings. It was suggested that we should set limits to the scope of our technology use. For instance, we could activate geotracking when we are trying to find a specific place, but then close it so we do not remain connected (and vulnerable) all the time. However, this is difficult to achieve in practice, since items like smartphones and applications like WhatsApp are often required to fulfill employment and social requirements.

In a very short time, many ideas that seemed to belong to science fiction such as planes, drones and smart phones have become reality. There is no doubt that AI is following the same path. However, we must remember that AI is based on data, which is now being collected everywhere. By all agreeing to share our personal data with Google and the likes to obtain various goods and services, we have opened a Pandora box giving many tools to cyber attackers, and we are not yet equipped to understand and deal with the consequences of this decision. As one panellist noted, "data is the new oil" and we must treat it accordingly.

In addition, there is no question that AI can be used harmfully. It has become rather easy to hack a smart device, change its algorithm and redirect it for malicious purposes. Because of the nature of this technology, cyberattacks involving AI have a much more dramatic impact than "traditional" cyberattacks such as phishing (we can think, for instance, about the consequences of hacking into autonomous cars). Wrongdoers may now even be able to control the human brain, which is the most powerful computer. Indeed, because our senses are too slow to transmit all the input and output received to the brain in a timely manner, we have developed sensors to capture this input in lieu of the senses. This can lead to wonderful innovations such as allowing blind people to see; yet it also opens the door to "brain hacking" and tricking people into doing things without their consent, or abuses by the military. AI is as powerful as it can be dangerous and panellists believe that we are currently underestimating its consequences. We must capitalize on what we have learned from previous experiences involving technology and find a way to regulate this newest technology before it is too late.

How to do so however remains a challenge, notably because the Internet is "glocal" and there is a bottom-up demand for regulation it in a way that reflects the values of different countries. One legislator cannot provide all the answers (for instance, privacy is not defined in the same way in every State) and this brings us back to the necessity of working collectively to achieve results. All panellists agreed that new technologies are also wonderful tools that allow us to achieve great things. We should remain optimistic and continue to use them for the greater good. We also need to keep raising awareness and institutionalizing concepts to be prepared for eventual cyberattacks involving AI and at least minimize, if not eliminate the dreadful consequences that such attacks can bring.

Justine Ferland, University of Geneva, August 20, 2018