**The 2012 CLSR-LSPI Seminar on Privacy, Data Protection & Cyber- Security – Presented at the 7th International Conference on Legal, Security and Privacy Issues in IT Law (LSPI) October 2-4, 2012, Athens**

|  |  |
| --- | --- |
| **Chaired by:** Prof Steve Saxby, Editor-in-Chief of Computer Law & Security Review (CLSR)  **[mailto: s.j.saxby@soton.ac.uk]**     ABSTRACT  This has been a big year for privacy with so much going on within the EU regarding reform of data protection. What are the implications of reform here and what are the issues that concern us about the proposed new data protection regime contained in the proposed Regulation? We hear a lot about the 'right to be forgotten'. How is that possible in the digital age within the online world? And what can be done about the big players who stand charged with the erosion of privacy viz Facebook, Google, Skype & YouTube etc? How can the law keep up with technological change when the latter is moving so fast eg with RFID, Cloud and social networking? To what extent can data breach notification, net neutrality and privacy impact assessment help and how should the law approach issues of liability and criminality in relation to privacy? What is the state of play too in the relationship between privacy policy and state surveillance and, given its implications for privacy, what obligations should governments adopt in response to cybersecurity regulation and data management? Is there a place for privacy self-regulation and if so in what respects and how effective are the Information Commissioners who often complain of being under resourced? In reviewing the way privacy law has emerged do we now need a completely new approach to the whole issue? Has the law crept into its present form simply by default? Do we need some new thinking now that reflects the fact that law is only one dimension in the battle for privacy? If so what are the other factors we need to recognise?  **©** 2013 Respective authors. Published by Elsevier Ltd. All rights reserved  Keywords: cyber-privacy; data security; data abuse; function-creep; privacy regulation; surveillance society; privacy by design; social media privacy; cyber-crime |  |

**Sibanda, Omphemetse, College of Law of the University of South Africa, [mailto:SIBANOS@unisa.ac.za]**

Omphemetse Sibanda is a Professor at the College of Law of the University of South Africa, and the Chair of the Department of Criminal and Procedural Law. His qualifications are: LLD in International Economic Law (University of North West); LLM (Georgetown University Law Centre); LLB (Hon) & B JURIS (Vista University, now the new University of Johannesburg). His academic and research interests are of an MIT nature, and include focus on e-governance; international white collar crime; international trade law and remedies; dispute resolution; and interface between trade law and human rights issues such as labour conditions and access to essential medicine. He has written and published a number of articles in academic journals, and presented papers at national and international conferences. He is the Unisa College of Law champion tasked with leading a group of subject experts to design a signature module on social dimensions of justice.

**1. Striking a balance between State piracy of personal data and protection of individuals’ cyber privacy**

My focus is on the developments in South Africa with reference to data collection and protection laws and regulations, and the ongoing debate about the South African government to clothe itself in complete privacy under the guise of State security, and its rejection of public interest clause in the Information legislation. My contribution anchors around these cardinal acknowledgements, namely:

1.    There are manifold risks to privacy associated with individual’s use of and participation in the internet environment

2.    That the right to privacy is internationally recognised as a fundamental right, including in recognition the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights, and other regional instruments;

3.    The South African Constitution, one of the few most progressive in the world, enshrines the right to privacy

4.    Data protection laws are closely linked to privacy laws

5.    There is no all-encompassing privacy or data protection legislation in South Africa.

6.    The use and disclosure of personal information by governments and corporations is the world’s deadliest threat to civil liberties and fundamental human rights and freedoms.

7.    The rapid growth and increasing use of the Internet give rise to many and complex privacy issues, which in turn involves other issues such cyber threats and cyber security.

8.    *Public accountability* may require outside access to personal information as part of democratic governance, and *bureaucratic rationality* may demand outside access as part of effective functioning of administrative organs.

A key talking point of my contribution will be to revisit of Paul Schwartz’s (2000) observations that “debate about Internet privacy has employed a deeply flawed rhetoric”. And most particularly the so-called (a) rhetoric that slights the State’s important role in “shaping both a privacy market and privacy norms for personal information in cyberspace”; (b) the “flaws in the leading paradigm of information privacy, which conceives of privacy as a personal right to control the use of one’s data”; and (c) the so-called “autonomy trap” of the advocacy of primacy of individual responsibility personal data use to the exclusion of nongovernmental intervention.

**Jochen Moeller, Vice President of the European Association for Data Media Security [mailto:** **eadms@kroeger-moeller.de]**

**Jochen Moeller** graduated in Engineering (Dipl. Ing.) in 1985 from the University of Applied Science Moenchengladbach, Germany. Until 1999 he worked in the International Machine Building and Plant engineering industry and regularly delivered lectures on the latest research and development subjects in these industries. Since 1999 Jochen Moeller has been working in the field of high security equipment and thus in close cooperation with different governmental organisations. In 2008 he was one of the Charter members of the EA DMS and now holds the office of Vice-President in this organisation, being responsible for all development and auditing. In this role he has been active as adviser to police, government departments and research institutes in different European countries.

**2. Protection of individuals and companies – the forgotten task**

The perspective of our association is very much driven by the experiences talking to victims of data theft and data abuse. We think data security and data protection can be structured in three different categories, state, business and private.

In the “state category” we are talking about attacks on states or governmental organisations or e.g. asymmetric attacks on infrastructure, called cyber war. Internet is the essential tool to make most of these actions possible. As long as attacks are fended off damages will be low. But a successful attack may have the potential to change the world.

In the “business category” we are talking about data abuse committed by well organised professional structures (legal and illegal). This economic espionage is often called cybercrime, although internet is only one of the tools in use. Conventional theft and abuse is at least as important. Economic damage is extremely severe but difficult to prove. The number of unreported cases is certainly also very high.

In the “private category” most data abuse (legal and illegal) is committed for marketing and sales purposes. The abuse is associated with strong mass marketing tools and the target is accumulated low profile abuses adding up to the intended e.g. profits or savings. In this category data mining and large data pools are vital for the success. The damage per attack may be low, but supporters of course need to hear about police successes and verdicts from time to time.

Governments seem to fully focus their efforts on the “state category”. Legislation is not considered to be relevant to reduce or control the dimension of these problems and should therefore mainly be used to assure full access to all data from all sources at all times.

In the “business category” responsibility is passed over to associations and companies. The philosophy is “buy yourself the degree of safety you need” and “create standards for easy orientation yourself”. But this philosophy will not provide legislation for a practical protection and chance to find compensation for damage.

In the “private category” governments seem to only feign action. Examples show a focus on temporary media awareness but no real understanding of problems and therefore possible solutions using legislation.

With the present focus of European governments a society comes closer, as described by Yevgeny Zamyatin in his famous book; “We”. But if legislation clearly points out who has the ownership of data at a particular time and provides strict rules as to how ownership can be transferred, protection of privacy and protection against economic espionage may still be possible. Governments must be encouraged to develop tools against war and terrorism, which are not dependent on super large data collections. Even huge data pools did not assist the GDR to survive.

|  |  |
| --- | --- |
|  |  |
|  | |

Tamar Gidron, Haim Striks School of Law

<mailto:tgidron@netvision.net.il>]

**Dr. Tamar Gidron** (LLB, Hebrew University, Law Faculty Jerusalem. Israel; LLM and Dr. Jur.: Tel-Aviv University Law Faculty Israel) is the Head of Dispute Management and Resolution Research Center, COMAS Israel and the Head of the Competition Law- Middle East initiative- Research Center, COMAS and The University of London. She was the Dean of the Haim Striks Law School College of Management Israel from 2000 to 2008. She teaches Tort Law, Defamation, Privacy, Economic Torts, Consumer Law.

**Uri Volovelsky, practicing attorney[mailto:uri.volovelsky@gmail.com]**

|  |
| --- |
| **Uri Volovelsky**, LL.M. Fordham University, New York (Banking, Corporate Law & Finance Law) (cum laude); M.B.A., College of Management Academic Studies, Rishon LeZion (Multinational Business Activities); LL.B., College of Management Academic Studies, Rishon LeZion (cum laude); B.A. Interdisciplinary Center, Herzliya (Government, Diplomacy and Strategy) (cum laude). Uri Volovelsky is a practicing attorney specializing in corporate and commercial law and international commercial agreements. Uri served as Deputy Editor and Academic Staff Member of the Hamisphat Law Review as well as Associate Editor of Fordham University's Journal of Corporate and Finance Law. In addition, Uri is a longstanding judge at the Philip C. Jessup "International Law Moot Court Competition". '  **3. Challenging the erosion of legal rights and interests in an online world of rapid change**  The extraordinary technological developments of recent years have created concerns regarding possible harm to rights and interests which the law seeks to protect, such as the right to privacy, freedom of information, the right of access to the courts, the right to reputation and copyrights.  Legal literature tends to regard technology and the law as enemies or as competitors. Often, the law is perceived as lagging behind technology. And indeed – in factual terms, the law by its nature responds to technological developments. The question, then, is which is the most appropriate institution (in terms of speed of adaptation and flexibility) to draw a balance between “vulnerable” legal rights and technology? Is it the legislature, or the courts which examine the technological developments from one case to another (that is, through the case law)?  One of the main points we wish to emphasize in this regard is the need to adopt a holistic perspective and a systematic "across the board" action in order to successfully cope with the main problems posed by new technologies. This means that all relevant "players" should join in a collective effort to adopt a comprehensive and systematic regime based on the following principles:  1) Encouraging consumers of technology to be more aware of and protective of their rights; Disabling Facebook’s facial recognition feature is a good example.  2) Encouraging providers of technology services and web site owners to conduct themselves ethically and ensure the greatest possible security of databases containing private information with the result that consumers will be more forthcoming about providing information; Avoiding "function creep" should be the norm.  3) Updating legislation – conventions, directives, state legislation – to meet the technological developments' challenge. Legal rules should be defined in a broad manner leaving the court judicial discretion to interpret the law, the conventions and the directives in a manner compatible with day to day life as well as in a manner which can contend with the inherent difficulty of foreseeing the full range of situations and questions ensuing from the rapidity of technological developments;  4) Providing the courts with wide discretion- the courts, which, in our opinion, have so far had the most under-appreciated job and which rarely have been spoken about or had their importance recognized- should, in our view, play a key role in any attempt to protect the fundamental rights entrenched in the law.  Following are some examples of Israeli law which illustrate the importance of the judicial role in protecting privacy and finding the right balance between conflicting interests in the field of technology in the modern era.  Defining legislation: two significant examples of legislation which might potentially infringe privacy have reached the Israeli Supreme Court for interpretation: The *Israeli Biometric Database Act* and the *Transfer of Communications Data to Public Authorities Act*, which was recently expanded. In both instances, the Supreme Court supported the legislature despite the possible infringement of privacy; however, the court left an opening for future reconsideration of the two statutes.  Defining key values- the courts have an important role in the interpretation of the concept of “privacy” and “private information”. It also has a role in determining priorities between the scope of protection of privacy and conflicting interests. The courts have the power to shape technology through the laws of evidence, such as "the fruits of the poisonous tree". They can also place conditions on evidence derived from a public computer network – using the “best evidence rule” and demand that parties wishing to present scientific data prove that is has been derived from a secure system that safeguards the privacy of the information stored within it.  The issue of anonymity of publications on the Internet raises another question: what is the best way to deal with the need to protect anonymity on the web – either as an aspect of freedom of speech or as an aspect of the right to privacy – when dealing with a person’s application to reveal the IP address of someone infringing his rights by publishing online? The Supreme Court recently rejected an application to disclose the IP address of someone who had severely defamed the plaintiff. The judgment attracted considerable criticism which focused on the question of whether this issue should really be regulated by legislation, even though that legislation could never catch up with the users who would find ways to conceal their identities, or left to the discretion of the courts which are able to respond quickly and produce an immediate effect on the behaviour of users. The decision as to who decides and in which way, must naturally take into account the injured party’s right of reputation and the right to access the courts on the one hand, and on the other hand, freedom of speech and privacy of the person posting on the Internet.  Courts are better equipped to successfully balance between opposing fundamental rights, mainly because courts have the power to set-up and adjust legal rules to different factual situations which in turn require wide range of solutions. By the flexibility to adjust their legal rule, courts can prevent a situation whereby setting up a broad range of list of circumstances under which the disclosure of online authors’ identity would be disclosed may cause a chilling effect deterring online publications. The legislation process on the other hand is cumbersome and time consuming, thus lack the required tools to properly meet the challenges created by technology.    ------------------------------------------------------------------------------------------------------------------- |

**Susan Corbett Victoria University of Wellington, New Zealand [mailto:Susan.Corbett@vuw.ac.nz]**

**Susan Corbett, Associate Professor of Commercial Law** School of Accounting and Commercial Law, Victoria Business School (VBS), *Orauariki*, Victoria University of Wellington, New Zealand. She is admitted as a solicitor in the UK and New Zealand and is an Associate of the Arbitrators’ and Mediators’ Institute of New Zealand. Her research areas include copyright law, E-commerce law, and cyber law. She has written and published a number of academic articles and presented papers at national and international conferences. She is currently writing a book on internet law and is also a member of an international research team which is exploring legal and technological means of preserving Australasian born-digital cultural entities for future generations.

**4. The difficulties of deleting information that has been made available online and the problems of relying solely on domestic privacy regulation.**

My overall conclusion is that, in the same way as the copyright regime requires international mechanisms for its enforcement, such as the Berne Convention and TRIPs, the most appropriate and practicable solution for online privacy protection must be provided by an international regime. There are many reasons why domestic privacy regulation is increasingly untenable in an online environment. These include the uses, both authorised and unauthorised, by other online agencies of information collected by one agency. Individuals whose personal information has been used, or misused, in this way cannot be confident that all versions of their information will eventually be removed - this will continue to be true even were all domestic privacy laws amended to include a compulsory deletion requirement. Versions of information about an identifiable individual which are stored on servers in different jurisdictions will not be subject to the domestic privacy law of that individual and, absent international reciprocity arrangements, any enforcement of privacy laws in those other jurisdictions by the individual is likely to be impractical.

The increasingly common use of cloud data storage facilities by agencies exemplifies the need for international privacy regulation. Many cloud services are not situated in the same jurisdiction as their customers and many cloud service providers explicitly disclaim all liability in regard to data protection. Although the contract between a customer and the cloud service provider may specify the law which is to apply to the contract and the jurisdiction in which disputes may be heard, this is not always the case. Furthermore, mainly because the customer has no real input into negotiating the terms of the contract with the cloud provider, there is no guarantee that the courts of the jurisdiction specified in the contract will agree that their jurisdiction is *forum conveniens* to hear a dispute. In addition, much domestic privacy regulation does not permit recourse to the courts.

Hence there will also, of course, need to be international dispute resolution processes for privacy breaches available. Unlike the dispute resolution process provided for trade-related intellectual property disputes under the auspices of the World Trade Organisation, privacy disputes will require a process that is more suitable for individual complainants. It should be economical, fast and easily accessible - somewhat akin to the online domain name dispute resolution processes that are overseen by country code top level domain name registrars, such as the .uk registrar, Nominet, and the .nz Domain Name Commission.

Another important consideration is that most domestic privacy laws, including the New Zealand Privacy Act, do not apply to personal information collected or held by an individual “… solely or principally for the purposes of, or in connection with, that individual’s personal, family or household affairs.” In today’s era of online social networking this exclusion is indefensible and should also be addressed by international regulation. Just as the intellectual property law regime relies upon international Treaties and Agreements which provide minimum standards and reciprocity provisions to which all states must adhere, so too the privacy regime must acknowledge the new demands of the online world of information.

**Alessandro Mantelero, Politecnico di Torino [mailto:alessandro.mantelero@polito.it]**

**Alessandro Mantelero** is Professor of Private Law at Politecnico di Torino, (Fourth School of Engineering Management and Industrial Engineering) and Faculty Fellow at Nexa Center for Internet and Society. He graduated cum laude in Law at the University of Turin on 1998. Ph.D. in Civil Law from the same University. He is author of numerous publications and is currently focusing his studies on data protection, ISP liability and legal implications of cloud computing and big data. Alessandro Mantelero was admitted to the Italian bar in 2001. He is involved in different national and international research programs and is Project Member at the Network of Excellence in Internet Science and co-director of Cloud Computing Governance Initiative for the Nexa Center. The Cloud Computing Governance Initiative has been launched by the Berkman Center (Harvard University) and involves the following universities and research centers: Harvard University (Berkman Center), Politecnico di Torino ( Nexa Center), Keio University and University of St. Gallen. In 2012 he was Visiting Researcher at Berkman Center for Internet & Society at Harvard University.

**5. Different regional approaches to data protection and convergence towards global data protection principles**

During the Seventies, different European countries adopted regulations on data protection with regard to public sector information, in order to tackle the risks of total control. These regulations also took into consideration the early data collection and merging activities that were carried out by the private sector in different fields. These were the early legal reactions to data collection, a phenomenon destined to grow exponentially in the following years, due to the introduction of new and more sophisticated technological devices that were able to manage and merge large amounts of data.

Looking to the present day, the aim of private data collection has not changed; information is still used for businesses in order to extract value from it, even if new technological tools have significantly increased the possibility of defining detailed personal profiles. By contrast, in the public sector, the emerging needs concerning public security induce agencies to require information from the private sector and merge this data with their own records, with relevant consequences in terms of social control. Finally, in the last few years, the paradigm of Big Data has generated a high concentration of power over information in the hands of big companies and government agencies thereby increasing the relevance of these issues, due to the predictive capabilities of Big Data management.

In this scenario, characterized by the central role and increasing value of information, it is necessary to adopt specific rules in order to regulate the information flow, define the rights over data and ensure adequate enforcement. This need concerns not only the protection of personal rights, but also assumes a relevance from a market point of view: clear rules and adequate protection reinforce individual trust in those who collect and process data and guarantee fair negotiation, avoiding unfair practices in the collection and use of data with negative effects on competition.

For these reasons, the first approach to data protection, based on different national regulations on specific aspects, is no longer adequate in a world where data flows across national boundaries many times per second and various private or public bodies collect information from different countries. Therefore general and common principles or regulations have been jointly adopted by countries in different areas of the world. In this way, different regional approaches to data protection emerged and are still emerging.

Among the various experiences, the EU model has a long tradition and has had a significant impact on the global system as many other countries have adopted legislations based on it. Now this model is changing towards a higher level of protection and a more homogeneous processing of data, which has been defined by the recent EU Proposal for a General Data Protection Regulation. The European Union could probably adopt a different strategy, with less attention to detail, maintaining the original structure of the Directive 95/46/EC focused on principles. A regulation based on principles and a supranational independent authority, which has the task of implementing them, would be more suitable in the context of a continuously changing world.

Looking to the other side of the Atlantic, we can see that big changes in data protection are also about to happen in the US. The American model is evolving towards a new model, which continues to differ from the UE and from the new European proposal, but represents the attempt to give an answer to the general global request for data protection coming from individuals.

In this field it is necessary to keep up constructive communication that will not remain solely between the EU and the US, involving not only the countries where the attention for these issues has a long history, but also the other nations where different data protection models are emerging, such as India and China, in order to gain a wider global convergence on the fundamental principles of data protection.

In defining these common principles it is important to avoid a race to the bottom that would focus the attention only on specific and limited aspects of data protection or a race to the top that would lead to a more protective model. A coherent and sufficiently strong model of data protection is necessary. On this basis every country -or rather every geographical area-, will build its specific rules, in coherence with its historical, cultural and legal system, but convergence on the principles and basic rules will facilitate data protection and data flow.

It is fundamental to transform the struggle between models into the interoperability between them and to ensure the respect for differences in a context of efficient data flow management, by means of international treaties and other forms of cooperation.

|  |  |
| --- | --- |
|  |  |

Henrik Tjernberg, Chairman of Micro Systemation (MSAB) [mailto:Henrik.Tjernberg@msab.com]

**Henrik Tjernberg** was born 1960 in the north of Sweden and studied Engineering Physics at the Royal Institute of Technology in Stockholm. In 1985 he became development manager at Micro Systemation AB, where he a year later became president and CEO. During the 90s Micro Systemation developed telecommunications software and in conjunction with its IPO in 1999 launched SoftGSM, the first ever entirely software-based GSM modem. Henrik Tjernberg was elected chairman 2002 and the company started the development of XRY, which is now the world's leading product for forensic analysis of mobile devices, mainly mobile phones.

**6. Privacy as an absolute value in the online world**

All citizens have the right to be presumed innocent until proven otherwise - This is the foundation on which Western legal tradition is based. It also implies that citizens should be treated as innocent and not be subjected to monitoring and data collection until a clear suspicion of crime exists.

This implies that states and governments must actively, by legislation, be prevented from collecting data on all of their citizens, regardless of motives. It is not until there is a reasonable suspicion of crime that data mining and direct surveillance may begin. Europe has chosen a different path and a very dangerous one. The Data Retention Directive is one example how pragmatism and supposed rationality leads EU to compromise on key rule of law and thereby undermining the public trust in law enforcement authorities.

The threat does not come from private companies, which, like Facebook, collects data about their users in order to build marketing databases. Users can choose to participate or not. The threat is states and governments, which with legislation will force these companies to provide information whenever the authorities wish. This is dangerous, inefficient and terribly expensive and threatens to destroy the open society as we know it. Did we tear down “that wall” just to import the DDR surveillance society? Democracy presupposes freedom of expression, privacy and a private sphere beyond society's control. Tools and methods that facilitate oppression of citizens must be avoided at all costs.

Privacy is an absolute value and must not be compromised by the “nothing to hide” argument. The individuals that got “nothing to hide” are in fact the biggest losers when integrity is expelled from the society.

The point here is that instead of collecting irrelevant information on innocent people the authorities should have powerful tools to gather information once a reasonable suspicion can be established.

The new digital world may give the law enforcements authority’s new effective tools to gather evidence and prevent crime. But it also presents governments the possibility of complete monitoring of their citizens. Let’s go the first way and skip the second.

Benjamin Franklin put it something like: *People willing to sacrifice freedom for security deserve neither and will lose both*.

I’m sure he was right.

**Note:** These comments are personal to the author and do not reflect the opinions of Micro Systemation (MSAB)

**Janine Hillier Pamplin College of Business, Virginia Tech, USA**

[**[mailto:jhiller@vt.edu]**](mailto:[mailto:jhiller@vt.edu])

**Janine Hillier** is Professor of Business Law at the Pamplin College of Business, Virginia Tech, Blacksburg, Virginia, USA. Dr. Hiller's teaching achievements include her designing one of the first Internet Law courses in the country. She currently teaches Internet Law and Policy to graduate students at Virginia Tech, to students at Thunderbird University and INT, France through distance learning. She has also co-authored one of the first textbooks on Internet Law. She has conducted seminars through the Management Development Office and has been a lecturer of Continuing Education Seminars for the Virginia Law Foundation. Dr. Hiller's research focuses on the challenges and policy issues of how traditional law and legal institutions can sufficiently address and accommodate the evolution of the advanced technological environment. Electronic commerce makes her research more complex, since it is international in nature, and therefore, international principles and norms must be considered. Research in electronic commerce and the law has included various aspects of relationships between electronic commerce and privacy, security and trust, and electronic government and privacy. Her research articles have appeared in American Business Law Journal, Banking Law Journal and Real Estate Law Journal.

**7. The future of privacy and security in an evolving framework**

Privacy and security issues of today and tomorrow are affected by rapidly advancing technology; this results in a type of “catch-up” by laws and regulations, which have as their aim the preservation of societal values. A few thought provoking ideas are offered as we think about the future of privacy and security. These ideas are not original, but discuss the evolving privacy framework and future possibilities.

First, communication technology has advanced so rapidly that our conception of privacy may change as a result. This is not to say that privacy as a fundamental right is evaporating or that we are giving up on protecting privacy; not at all. However, the way that we share information, and the unpredictable ways that technology will allow us to share information in the future requires us to think about what the fundamental right to privacy means, and how reasonable expectations of privacy are defined. Individual and societal conceptions of reasonable privacy may be evolving.

Second, in an era of evolving technology the globally accepted Fair Information Privacy Principles (FIPP) may not be sufficient to protect individual privacy; recent studies and frameworks reflect the changing environment.

See: ftc.gov/os/2012/03/120326privacyreport.pdf The technology may be advancing beyond the individual’s ability to control the information, which is the hallmark of the FIPP. The collection of information at Internet speed, the aggregation of that information, and ubiquitous consumer use of the Internet, are some of the factors that create an environment of rapid and more complex transactions that may thwart the power of the individual to control the collection and/or use of personal information. The US Federal Trade Commission’s March, 2012 Report, “Protecting Consumer Privacy in an Era of Rapid Change” reflects some of these concerns and proposes the adoption of best practices, including Privacy by Design principles.

Privacy by Design (PBD) is not new; for example the Ontario, Canada, Information and Privacy Commissioner’s Office has been one of the agencies promoting the concept for a number of years. One of the foundational principles of PBD is that protecting privacy is not a “zero sum” game; in other words one may have privacy and security when both principles are designed into the system architecture from the beginning. This is also related to the proposition that perhaps we should rethink the language that we use when we discuss *balancing* privacy and security. Using a balancing scale means that when one side is favored the other side necessarily loses, and this usually means privacy. PBD proponents argue that this does not have to happen; one may have privacy as well as security. While the details are beyond the scope of this discussion, PBD includes the concepts that privacy protection can be incorporated into systems proactively and as a default, and that both procedures and technologies are important in this process.

As technology continues to change the way that we interact with each other and the world, it is important that our conceptions of privacy and security evolve as well, and that we continue to protect our fundamental rights and principles. Technology, when designed with these rights in mind, has the potential to protect privacy as well as provide security.

**Wian Erlank, North-West University, Potchefstroom, South Africa** [**[mailto:Wian.Erlank@nwu.ac.za]**](mailto:[mailto:Wian.Erlank@nwu.ac.za])

**Wian Erlank** studied law at the University of Stellenbosch where he obtained his LLB degree in 2002. This was followed with an LLM in international trade law in 2004. He has just finished his LLD dissertation entitled "Property in Virtual Worlds. During the course of his studies he also obtained a BA Honours in classical literature from Stellenbosch, as well as a Certificate in Legal Practice from the UNISA College of Law (with distinction). He was admitted as an Advocate of the High Court of South Africa in 2008. After lecturing at Stellenbosch University he was appointed as lecturer at North-West University in 2011 where he has taught and currently teaches land reform, research methodology, legal skills and property law. He is currently a senior lecturer at North-West University. He spent 3 years as a permanent doctoral candidate and researcher at the South African Research Chair in Property Law and there obtained expert knowledge of national, international and comparative property law as well as the constitutional aspects thereof. His areas of expertise include property law, IT law, virtual property law and space law. He has also published in these areas and regularly presents papers at both national and international conferences. Apart from being and advocate and lecturer he is also a member of the Association for Law, Property and Society (ALPS), Young Property Lawyers Forum (YPL), Academics Promoting the Pedagogy of Effective Advocacy in Law (APPEAL) and an associate of the Centre for Constitutional Rights (CFCR).

**8. The move of various virtual world operators as well as large social media companies to institute a so-called real/verified user id system.**

In the past few months we have seen an interesting phenomenon in the area of online identities. While the *de facto* situation in the past has been that online accounts are normally anonymous, or else possibly verifiable at the whim of the account creator; there has been no real need for, or attempt to be able to link an online identity to the identity of its creator in the real world. However, this has now changed and we are seeing that it is becoming more commonplace to have online identities that are publicly and verifiably linked to someone’s identity in the real world. For example, Google has moved in this direction with the usernames and accounts in YouTube where users have been given the opportunity to link their YouTube accounts and profiles to their verified Google identities. Although I initially expected a huge public outcry, it would seem as if the voluntary basis of the move has ensured that the adoption of this has been well-received.

This, of course, has both pros and cons. On the positive side, A move towards online identities being publicly verifiable will have a direct result in diminishing the amount of spam and nonsensical comments that are encountered all over the web. It will also help with curbing such modern societal problems such as cyber bullying, child pornography, identity theft and anonymous slander. However, on the other side of the coin, if one did not have the option to create anonymous accounts anymore, some of the most important aspects of the internet will be lost. Repressive governments will be able to target whistle-blowers and dissidents with impunity and the free flow of information will be disrupted. We have witnessed how powerful the use of social media is in bringing about the Arab Spring. This would never have been possible if it was an absolute requirement that every online account must be verified.

Another area where the verification of online identities could be beneficial is when one deals with virtual property. Since an online account is one of the objects of virtual property and usually has value (either monetary or sentimental), it will be beneficial if the owner of such virtual property can be accurately identified in instances such as designing on the inheritance of virtual property in a deceased estate, or even for using virtual property for collateral in obtaining loans in the real world. When dealing with virtual property, one does not need the online account to be publicly verifiable (which could diminish the entertainment effect of game-based virtual worlds), but it should at least be verified with the developer/ provider of the service.

To briefly summarise some options of how online verification should be approached. For some online services and especially certain social media applications like Facebook, which relies on and in fact thrives on the veracity of an online identity, this would be a logical and beneficial move. However, for general interaction on and with the internet, there should always be the option to have an unverified account for promoting free speech and the widespread dissemination of information, without restriction, sanction or censoring by governments.

**Gönenç Gürkaynak, İlay Yılmaz, Derya Durlu of ELIG, Attorneys-at-Law Istanbul, Turkey**

**Gönenç Gürkaynak** **[mailto:** [**gonenc.gurkaynak@elig.com**](mailto:gonenc.gurkaynak@elig.com)**]**

**Gönenç Gürkaynak** holds an L.L.B. degree from Ankara University Law School (1997) and an L.L.M. degree from Harvard Law School (2001). He is a qualified attorney of the Istanbul Bar (1998), the New York Bar (2002), the Brussels Bar (2003), and he is also a Solicitor of the Law Society of England & Wales (2004). Gönenç Gürkaynak has been practicing as an attorney in Istanbul, New York, Brussels and again in Istanbul since 1997. He is one of the founding partners of ELIG, Attorneys-at-Law in Istanbul, which happens to be a leading Turkish law firm with 37 lawyers. In addition to frequently lecturing at three universities in Istanbul, he also holds a permanent teaching position at undergraduate and graduate levels at the Bilkent University Law School in Ankara, where he has been teaching since 2004. Gönenç Gürkaynak heads the Regulatory & Compliance department at ELIG, Attorneys-at-Law. He has had over 80 international and local articles published in English and in Turkish on various fields of law, including competition law, anti-corruption and corporate compliance matters, Internet law and IT law, and employment law and litigation, and two published books, one on competition law, published by the Turkish Competition Authority, and the other on "Fundamental Concepts of Anglo-American Law".

**İlay Yılmaz [mailto:** **ilay.yilmaz@elig.com]**

**İlay Yılmaz** is an associate at ELIG, Attorneys-at-Law. She graduated from Dokuz Eylül University Law School in 2003, where she was admitted for her undergraduate studies in 1999. She began her career in the field of contracts, commercial law and litigation in 2005. İlay Yılmaz was admitted to the Ankara Bar in 2005 and is currently admitted to the İstanbul Bar. She has represented various multinational and national companies before the Turkish authorities. She has worked on their compliance to the laws, contracts, commercial law, Internet law, IT law, energy market law; conducted litigations and settlement processes; has provided consultancy and given numerous legal opinions to the clients on various fields of Turkish legislation; and she has an extensive experience in these areas. She is the co-author for Turkey chapter of two books; “*Data Protection & Privacy - Jurisdictional Comparisons*” published by The European Lawyer Ref Series, and “*Litigation & Dispute Resolution 1st Edition*” published by Global Legal Insights.

She is fluent in English.

**Derya Durlu [mailto:** **derya.durlu@elig.com]**

**Derya Durlu** is an associate at ELIG, Attorneys-at-Law. She holds an LL.B. degree from Bilkent University Faculty of Law. She is qualified to practice in the Istanbul Bar. Ms. Durlu has experience in representing multinational companies and large domestic clients on competition law, internet law, IT law, corporate compliance matters, and general corporate and contracts law. She is the co-author and co-editor with Mr. Gonenc Gurkaynak of a book published by Legal Publishing: “A Discussion Book to Induce Socratic Questioning and Learning of Fundamental Concepts of Anglo-American Law”.

**9. The Interface between cyber-security and the right to privacy from the Turkish experience Perspective.**

The right to privacy underpins some of the fundamental values human rights are enshrined upon. These include freedom of speech, freedom of association, freedom of thought and many others that now form an inalienable part of the constitutional frameworks of civilized countries. The intersection between cyber-security and the “right to be left alone,”[[1]](#footnote-1) as Justice Brandeis stated in 1890, is a topical discourse that Internet law practitioners as well as scholars today should pay particular attention to.

Given the nascent legal framework regulating this field of law in Turkey, the cross-over of legal and ethical issues concerning the Internet in protecting the privacy of public figures and national security merits particular focus from the Turkish law perspective once the right to privacy intersects with cyber-security.

The topic is narrowed down below to address two primary issues from the Turkish legal experience: data privacy in relation to the use of mapping services in Turkey and privacy of politician’s personal lives.

**9.1. A look at data privacy in the use of online maps (such as Google Maps)**

There is a controversy of keeping military, governmental and police offices from being visible on mapping services as legal issues on protecting secret locales for national security reasons arise under Turkish law.

Law No. 657 on General Command of Mapping sets out the general provisions with respect to the functioning and duties of the General Command of Mapping (“GCM”), which is responsible for the official topographical mapping of the country in hard-copy and digital forms for military, government, administrative, educational uses.

Addendum Article 3 to Law No. 657[[2]](#footnote-2) sets forth that upon obtaining compatibility approval from the GCM, printed and numeric all kinds of land and air maps, atlas, sphere, and any document containing maps and information on maps (“Maps”) may be published, distributed or broadcasted for 5 years without being edited. If there is a change to be made on the Maps or if the GCM announces a change to be made on the Maps and in any case after the elapse of 5 year period, such amended Maps shall be sent to the GCM to obtain compatibility approval.

All maps and satellite imageries to be broadcasted by the online maps owner in Turkey are subject to the compatibility approval to be obtained from the GCM. Consequently, online maps owner is required to make sure that maps and satellite imageries to be licensed from third party providers and to be broadcasted in Turkey have been approved as compatible by the GCM.

Persons, who publish, distribute or broadcast Maps without obtaining compatibility approval from the General Command of Mapping shall be subject to judicial monetary fine as per the Turkish Criminal Law (Article 52).

Given the tension between national security and privacy of individuals, the extent of governmental exposure can be limited if sensitive information pertaining to the government/military and broadcasted through mapping services jeopardizes national security. However, the matter of how far should data protection laws and privacy regulations protect sensitive information relating to the government and military, but equally exposing individuals’ and private companies’ information is one that should be left to policy makers.

Requesting removal of information that is not public may be based upon specific privacy guidelines of mapping services (such as Google Maps), Law No. 657 (Addendum 3), national data protection provisions and other relevant laws. Companies are to fully (or partially) comply with governmental removal requests to remove texts, visuals and borders of military areas (particularly with respect to the visibility of “forbidden” territories due to national security reasons).

**9.2. Removal requests of hidden camera footage of a politician’s affair**

During April - June 2011, hidden camera footage of a Turkish member of the parliament was broadcasted on YouTube, subsequently followed by numerous removal requests of these contents from the respective MP, the Turkish Telecommunications Authority, as well as the political party to which the MP was affiliated. The hidden camera footage explicitly showed the MP having sexual intercourse with a woman. There were two court orders in relation to the removal of this content from YouTube. Obscenity was the legal basis of these court orders; however, the correct legal grounds for removal of such content should have been the violation of personal rights.

“Confidentiality of personal data” and “privacy of private life” as understood under Article 20 of Turkish Constitution, and politicians and other individuals are not separated in terms of protection of personal data and privacy of personal life.

**Arnaldo Sobrinho de Morais Neto, Brazilian Military Police, Brazil [mailto: asmn10@yahoo.com.br]**

**Arnaldo Sobrinho de Morais Neto**, is Lieutenant Colonel of the Brazilian Military Police. Master of Law by Federal University of Paraiba. Professor of the IESP College in Joao Pessoa, where teaches Criminal Law and IT Law. Researcher associated and executive Coordinator for Brazil of the International Association of Cybercrime Prevention (France). Researcher associated of the International Law Association - ILA (Brazilian branch). Is currently Executive Director of the Penitentiary System of Paraíba, also Penitentiary Council State - member.

He spoke about his research on cybercrime in Brazil, where he served in the fight against organized crime gangs.

1. Earl Warren and Louis Brandeis, “The Right to Privacy”, 4 Harvard Law Review 5, p.31 [↑](#footnote-ref-1)
2. “*For the purposes of preventing preparation and use of maps that are not in compliance with the interests of the country and that may be exploited in the international arena, public or private entities or real persons are obliged to obtain compatibility approval from the General Command of Mapping.*” Although Addendum Article 3 requires that in case of each and every change to be made on the Maps the revised Map shall be submitted to the GCM for compatibility approval, such a requirement should not be applicable for user generated content to be tagged or embedded on the Maps since the original map or the satellite imageries will not be changed and such user generated content may always be removed or blocked if it violates applicable laws or if it breaches the terms of service for the product. [↑](#footnote-ref-2)