|  |  |
| --- | --- |
| **THE 2013 CLSR-LSPI SEMINAR ON ELECTRONIC IDENTITY – THE GLOBAL CHALLENGE**  **Presented at the 8th international conference on Legal, Security and Privacy issues in IT Law (LSPI) November 11-15, 2013, Bangkok, Thailand**  **Date:** 12 November, 2013  **Venue:** Tilleke & Gibbins International Ltd. Bangkok, Thailand  **Seminar Chair:** Professor Steve Saxby, Editor-in-Chief, CLSR, s.j.saxby@soton.ac.uk |  |
| **ABSTRACT:**  We are the middle of a global identity crisis. New notions of identity are made possible in the online world where people eagerly share their personal data and leave ‘digital footprints'. Multiple, partial identities emerge distributed across cyberspace divorced from the physical person. The representation of personal characteristics in data sets, together with developing technologies and systems for identity management, in turn change how we are identified. Trustworthy means of electronic identification is now a key issue for business, governments and individuals in the fight against online identity crime. Yet, along with the increasing economic value of digital identity, there are also risks of identity misuse by organisations that mine large data sets for commercial purposes and in some cases by governments. Data proliferation and the non-transparency of processing practices make it impossible for the individual to track and police their use. Potential risks encompass not only threats to our privacy, but also knowledge-engineering that can falsify digital profiles attributed to us with harmful consequences. This panel session will address some of the big challenges around identity in the digital age and what they mean for policy and law (its regulation and protection). Questions for discussion include: What does identity mean today? What types of legal solutions are fit for purpose to protect modern identity interests? What rights, obligations and responsibilities should be associated with our digital identities? Should identity management be regulated and who should be held liable and for what? What should be the role of private and public sectors in identity assurance schemes? What are the global drivers of identity policies? How can due process be ensured where automated technologies affect the rights and concerns of citizens? How can individuals be more empowered to control their identity data and give informed consent to its use? How are biometrics and location tracking devices used in body surveillance changing the identity landscape?  **Keywords:** *digital identity; electronic identity; identity crime; managing online identity; big data; mobile identity; automated identification; identity surveillance; biometrics*  © 2014 the individual speakers. Published by Elsevier Ltd. All rights reserved. | |

**PANEL DISCUSSION THEMES**

|  |
| --- |
| The format of the seminar was a number of short presentations (around 5-7 minutes each) followed by a panel based question and answer session, giving members of the audience the chance to contribute and provide both answers to the questions posed but also allow the audience to raise further questions and help develop a way forward. A summary of the seminar topics and of the individual presentations dealing with those topics now follows.   1. **IDENTITY IN THE DIGITAL AGE: WHAT IS IT AND WHY DOES IT MATTER?**   The objective of this part is not to search for a single answer to the ultimate question, 'what is identity?', but rather to present and gather different views to help explore the modern meaning of this concept.  Possible discussion points include:   * What do we mean when we speak of identity in the digital age? Do we mean different personas that we adopt for different purposes, e.g. an individual may create one particular identity in relation to online dating, a second for their professional profile and another for anonymous blogging? Alternatively, do we mean a single 'real' identity, such as the one that we authenticate in online banking, existing simultaneously offline as well as online? * Is identity just a sum of external attributes by which we are capable of differentiation from other people, or does it have wider connotations? * What value can we extract from conceptualising identity from multidisciplinary perspectives (such as philosophy, biology, psychology, and sociology)? * What are the challenges of the fact that identity may mean different things in different contexts as increasingly evident online? For example, business notions of identity may be attached or assigned to a particular corporate perspective on an individual's identity, while different types of personal information are made available and gathered - sometimes covertly - in different online spaces (such as on social networks, in online stores and e-government services). Identities can also be chosen or imposed, or, more typically, a hybrid of the two. * How are digital representations of personal characteristics changing our notions of identity linked to the ways in which we identify individuals? For example, as digital identities become divorced from physical clues, prospects for identification of the ‘real’ person may not necessarily relate to our names anymore but subsist in new forms, such as in our search histories, IP addresses and targeted advertisements visible on our screens. Simultaneously, while some types of identities change only very gradually over a lifespan (for example, appearance); others have the potential to change quickly (for example, passwords).   **Commentator: Dr Clare Sullivan, *Lecturer in the School of law Division of Business University of South Australia [clare.sullivan@unisa.edu.au]***  *Dr Clare Sullivan is a cyber-law lawyer and faculty member at the School of Law at University of South Australia. Her research examines whether the digital identity that people use for transactions is emerging as a new legal concept, its legal nature, and how digital identity can be legally protected. The research has implications for a number of legal areas particularly the emergent right to identity and its relationship to the right to privacy. In 2011/12 Dr Sullivan was awarded a Fulbright scholarship to examine the legal implications of digital identity and cyber security under US and international law, which built on Dr Sullivan's earlier comparative research in Australia and Europe. Her book 'Digital Identity: An Emergent Legal Concept' is the first detailed legal study of digital identity and its implications for individuals, businesses and government. Dr Sullivan also co- authored the first report on trade-based money laundering for the Australian Institute of Criminology which was published in 2012. Dr Sullivan has authored a number of internationally published articles on digital identity and cyber security including the research she conducted in the UK, Europe and the US.*  We are now in an era where digital identity is central to accessing information and services. Digital identity is an identity which is composed of information stored and transmitted in digital form. Typically, the set of information required for transactions consists of full name, gender, date of birth and at least one piece of identifying information such as a signature or a numerical identifier. This identity will soon be the primary means of transacting as governments around the world move their services and transactions to digital format.  This new approach is necessarily based on the premise of one person: one digital identity. While one person: one identity is not a traditional legal requirement, nor has it been essential for private schemes like Visa credit and debit card transactions for example, it is now a necessary part of transacting. To address fraud, verification of digital identity is essential. Consequently, an individual can legitimately have only one digital identity under this type of scheme.  Furthermore, even if it is not a stated objective, the digital identity used for government services will also likely set the standard for transactions with the private sector. In effect, this means that the digital identity for government transactions becomes the individual’s digital identity. That digital identity becomes the primary means by which the individual is recognized and can enter into transactions in the virtual world.  In this context, there is an important distinction between identification and identity. Identification is just one part of the two processes to establish identity for a transaction. Although digital identity may seem to be just a modern version of having to provide identity papers, there is an important difference in the role played by human beings and information. Digital identity does merely not support a claim to identity. Digital identity is the actor in the transaction – it actually enables the dealing. This function distinguishes the functional role of digital identity from traditional identification procedures and processes.  As a set, the information which comprises digital identity has the critical role in the transaction, not the individual. The system looks for a match between the information presented and information on record. If there is a match, the system then automatically transacts with that digital identity.  These developments mean that it is inevitable that a digital identity will be necessary for an individual to fully function. This is evident now. In some countries digital identity is required for most government and private sector transactions. Estonia is a notable example. Other countries like the United States and Australia for example, are progressively moving government services and transactions to digital format. But even in transitioning countries, while it may seem that it is still possible for an individual to transact outside the digital system; this is increasingly not the case. For example, in many countries a paper tax return can still be lodged by a citizen instead of filing on-line using the e- tax portal. However, in reality, all data must be entered into, and processed by, the digital system. The individual who lodges a paper return is automatically assigned a digital identity by the system and the information on the document is scanned into, and processed by, the digital system.  This is a fundamental change and it is well underway. It is elevating identity to an unprecedented level of significance; and is set to transform the commercial and legal landscape.   1. **IDENTITY TO IDENTIFICATION: HOW SHOULD WE MANAGE AND REGULATE DIGITAL IDENTITIES?**   Combating rising levels of identity-related crime is an issue placed squarely on the agenda of policy makers wishing to encourage citizen engagement with the online domain. Business too is under increasing pressure to find secure but useable identity management tools. Yet, introducing trust in digital identity is challenging in an electronic space where traditional face-to- face mechanisms cannot operate. Technological advances such as encryption and digital signatures have partly met such challenges, but neither provides a perfect solution. Moreover, the widespread use of multiple identities in different digital contexts - with varying levels of verification, pseudonymity and anonymity desirable - is likely to give rise to new demand for services and tools. At the same time, identity management raises questions about the fair attribution of liability for identity breaches.  Possible discussion points include:   * Where should responsibilities and liabilities lie? For example, if it emerges that a bank is relying on compromised security mechanisms and is not delivering expected levels of protection, what implications should this have for its liability? * What role should public policy have in the provision of trusted digital identity assurance? * Will it remain possible to function effectively in society in the future without a digital identity? * To what extent can, and should, identity management be regulated? * Are privacy protection and self-regulation by online service providers compatible?   **Commentator: Dr David Newlyn**, ***School of Law, University of Western Sydney***  ***[d.newlyn@uws.edu.au]***  *Dr. David Newlyn (BEd (Hons) Wollongong University, LLB Sydney University, PhD Wollongong University) is a member of the academic staff in the School of Law at the University of Western Sydney. He has an extensive history of engagement within the fields of education and law. He teaches and researches in the areas of Business Law, Contract Law, Constitutional Law, and Legal Education. He has particular expertise in the area of electronic commerce.*  Although likely to increase in the future, in May 2013 Intel estimated that almost 640000 GB of Internet Protocol (IP) data was transferred through the online world in just one minute.[[1]](#footnote-1) A significant amount of this was either directly or indirectly linked to our individual digital identities. Given that at its most basic level a digital identity is a representation of, a proxy for or a supplement to the actual or real identity of a person or an organisation, identity management or access management is the systematically process of regulating access to information assets via a centralised policy based control of the establishment of the identity itself and the security of the storage of data associated with that identity.  There is increasing evidence that society is concerned about issues of identity security, privacy and the potential misuse of personal information. Fundamentally these concerns undermine trust and confidence in online services. If users cannot be assured that the information they provide is safe or that the identity of a person or business that they wish to deal with is beyond reproach, there will be an increasing reluctance to provide sensitive data or a failure to trust in the mechanisms for establishing identity in the online environment. Ensuring the safe, secure and transparent use of data will, therefore, be key to securing the success of identity management services.  The 2011 report into *Digital Identity Management: Enabling Innovation and Trust in the Internet Economy[[2]](#footnote-2)* prepared by the Organisation for Economic Co-operation and Development (OECD), notes that the potential growth in the digital economy is enormous. But in order to unlock this potential and to ensure the success of digital identity management, policy makers need to strive to achieve uniformity and consistency across relevant legal instruments, ensure transparent and consistent rules for privacy and security and minimise the costs of implementation and compliance costs for business. This will involve considerable efforts on the part of relevant stakeholders.  Although there are some standards relevant to digital identity and digital identity management already in existence, including those typically managed by international agencies such as the International Organisation for Standardisation (Eg. ISO/IEC 24760: A framework for identity management and ISO/IEC 29115: Entity authentication assurance framework), at present there appears to be little universal formal regulation in this area, this means that the problem becomes rather complex as it involves technical, social and cultural issues.  The possibilities to achieve universal management of identity systems involve either the use of the private sector or government regulation. In the case of the private sector, there are already some examples of this occurring in the area of financial securities (credit/debit cards) which are regulated by consortiums such as Europay, MasterCard and Visa (EMV) and the Payment Card Industry Security Standards Council (PCI). These may provide a useful guide to how such a system could be used on a much wider and completely global basis.  Or it could be that an international approach is needed via governments taking an active role in developing law which could universally regulate this area (such as the National Strategy for Trusted Identities in Cyberspace (NSTIC) from the USA and the Identity Assurance Programme (IDAP) from the UK). Given that digital identity and its management is both an international and a local matter, the international approach may be preferable to a private segmented/industry based approach, but such an approach would need to be aware of complex and changing technical, social and cultural issues which may be present now and in the future. The developed law would need to be all encompassing and include a clear set of guidelines as to responsibility for the protection and management of the data and the consequences for failure to adequately prepare that data and/or to store it correctly. At present this may be covered under existing breaches of contract law or negligence in some countries, but in the case of future government intervention it may be appropriate that the government includes specific provisions to deal with this matter. If this was not done in a universal fashion there may be problems in determining the relevant law of the forum which could prove problematic for individuals in accessing justice.  Currently the issue of the management of digital identity does not appear to have reached the level of maturity required to ensure the true economic potential of the internet, but given the rapid nature in which digital technology has been evolving it is critical that this issue is dealt with in a comprehensive and consistent fashion without further delay. Such a level of maturity will instill confidence in users that their data and identities are safe and once a universal approach is developed it can always be adapted for future needs as the relevant technology develops further.   1. **WHOSE DATA IS IT ANYWAY?**   Personal data, the raw material for this digital age, has become a valuable economic asset. Monetisation of digital identity leads to tension around the topic of control over our data (by whom, to what extent and for how long is it being controlled?). Legal concerns focus on issues such as ownership of and access to our data, including the potential application of intellectual property rights, not just in life but also in death. For example, in the US, lawsuits have been filed that seek to allow the transfer of a person’s ‘digital archives' (such as those belonging to a soldier killed in action) down generations of their family. How can, and should, the law protect us from those who would misuse our identity?  Possible discussion points include:   * Are new legal concepts around digital identity required in light of the substantial economic value now attributable to personal data? * Is it useful to consider identity data as property grounded in property rights acknowledged by law (such that its use – legally and illegally - should be compensable)? * What links may be made between the assertion of intellectual property rights and identity? Should there be intellectual property right in human identity or in profiles? What type of model would be most suitable (such as an extension to personality rights over one’s image as recognised in US law)? Are there any negative side effects to the proposal of an intellectual property framework for identity that we should anticipate? * Identity interests are seen traditionally as obtaining protection through rights to privacy and data protection law. Are these outdated now that? Should we have an explicit human right related to protecting the integrity of our identity enforceable in law? Is a more flexible model preferable to a prescriptive approach, such as normally associated with data protection rules? * Should law treat genetic data differently in terms of identity and personal data rights?   **Commentator:** **Ronald C. Griffin** is ***Professor of Law Emeritus, Washburn University, Topeka, Kansas and Professor of law, College of Law, Florida A&M University, Orlando, Florida.* *[Ronald.griffin@famu.edu]***  *As a visiting professor of law at Queens University in Kingston, Ontario, Professor Griffin served as a scholar and consultant in the specialized field of international trade and sales. He was invited to observe the hearings of the Meech Lake Accord, Canada's process for reconstructing its Constitution. His international study of law and culture has also included extended visits to Scotland, Ireland, South Africa and Japan.*  America is powered by science, energy and commerce. There is a physical world and a virtual world. The former accommodates things, weights and measures, and Cartesians. The latter accommodates avatars, digital replicas of the instruments we use in business, and war games that make death impermanent.  The United States occupies space in these realms. The government is its deputy. It roams in both to police the mavericks. There are catchy adverts for the country and a veneer for public consumption (we’re an open society). Beneath this fluff is a bureaucracy with ultra conservative values. It dredges our lives in wily ways, sifts through people’s habits, and mixes bits with its algorithms to determine whether somebody is a threat to society.  There are legislative rights (edicts bubbling up from the legislature that corrects things in the here and now) and legal rights (propositions individuals enforce on demand.) These rights (all of them) are trumped by the strands that knit us together as human beings.  There are realms for knowledge and commerce in this place. People in the knowledge realm lob ideas, science, and history at each other to find truth, order, certainty, and predictability. Practical men occupy the other realm. They scour landscapes to eke out an existence.  Most folks pack morals and ethics and heed them in their daily lives. They have a notion about privacy. It is a wall, they think, between the public and their families. In the 21st century it is something else. It is communing with everybody with the option to withdraw from communion to (1) invent and innovate, (2) control the flow of information, and (3) veil some things as secrets.  When a person puts his image and bits of his personality into cyberspace, as regards the image and bits, he lost his right to privacy. There are hard questions to be addressed. The answers control what people can read about other people. Was the information something an individual could protect? Did the victim shield or try to shield the data from the public? Did the internet service provider or online service provider (collector) have the option to disclose or not disclose material to somebody? Were the collectors under contractual or fiduciary duties “not to disclose the information”? Did they commit a breach? Were the victims’ celebrities or public figures? Was the information gossip (something we tolerate), news (facts, accounts about historic events, or something else uplifting), or both?  On the privacy front it is not about making privacy better per se. It is about compiling data about how people get on in their particular situation and how an individual might fare on his own. Here are some suggestions.  (1) We could disable Facebook’s facial recognition features.  (2) We could get internet service providers and online service providers to adhere to a code and pay fines for violations.  (3) We could put an international regime in play to constrain what people get to know.  (4) We could get the Federal Communications Commission to establish a code that lays out what internet service providers can share with security agencies; how transmissions are made to them; notice to others about transmissions to security agencies; a provision investing internet users with the “whatever” to get ISP’s to erase internet traces of someone’s user habits; and last, but not least, fines of not less than $170,000 for each violation of the user’s rights.   1. **INTERNATIONALISATION OF IDENTITY**   The Internet is a borderless domain, while the trend for globalisation calls for standardisation and convergent solutions. These two factors, together with the increasingly common use of cloud data storage situated in multiple jurisdictions (including cross-border data transfers and disclosures) suggest that the best solution for identity protection might be an international regime. Yet identity policies vary significantly across countries and legal cultures, which suggest that localised and culturally sensitive solutions are preferable. This tension leads to challenges. Can we have convergence on the principles of identity protection and global standards, such as through international forms of cooperation, or is significant divergence inevitable?  Possible discussion points include:   * How are concepts of identity and identity protection affected by globalisation? * What are the technical, social and legal challenges associated with achieving interoperability between online identity management across borders, together with harmonised governing legal systems? For example, the EU has launched its 'STORK 1.0' (Secure idenTity AcrOss BoRders LinKed) project to promote mutual recognition of national electronic identities (‘eIDs’), enabling EU-wide citizens to access electronic public services securely in other Member States. * Many cloud service providers disclaim data protection liability. At the same time, different approaches are been taken by national regulators (such as those in the EU, US and Australia) to reform their data protection regimes as they apply to cross border data. Are the two compatible?   **Commentator: Mpakwana Mthembu *(BJuris, LLB- University of Zululand; LLM (Specialisation in Commercial Law) - University of South Africa; LLM (Specialisation in Mercantile Law)- University of Pretoria, is a Senior Lecturer in Corporate Law in the Department of Mercantile Law, College of Law, University of South Africa [Mthemma@unisa.ac.za]**[[3]](#footnote-3)***  *Mpakwana is an admitted advocate of the High Court of South Africa. Her research is on Labour, Banking, Technology and Corporate Law***.**    In recent years, with the growing popularity of globalisation and cloud computing, data protection, data control, online identity, online privacy and data storage have become important issues. The topic is narrowed down to address the impact of globalisation and cloud computing on identity. The concept of ‘globalisation’ is used widely to sum up today’s world order. Globalisation is itself a term whose meaning is not clear and over which substantial disagreements exists among those who use it[[4]](#footnote-4). It means different things to different people. It can be used so broadly that it embraces everything and therefore means nothing.[[5]](#footnote-5) Globalisation allows for increased movement and border crossing, which permits the exchange of goods, services, ideas and practices. Although globalisation broadens the scope and opens new horizons for an increasing number of people from divergent origins, it has its evident shadow sides.[[6]](#footnote-6) Globalisation is alleged, to destroy personal identity, which is seen as reliant on sharply delineated differences among cultures.[[7]](#footnote-7)  Conversely, the increasingly common use of cloud computing storage demonstrates the need for international privacy regulation. It pertains computing with a pool of virtualised computer resources, hosting different workloads.[[8]](#footnote-8) Cloud environment as being borderless in nature, it does not allow for the use of single access control mechanisms and single language policy. [[9]](#footnote-9) Each cloud service provider (CSP) has its own access control mechanism and is not situated in the same jurisdiction.[[10]](#footnote-10) Currently users are obliged to use diverse access control mechanisms to secure their data stored at different CSP’s and they do not have an input into negotiating the terms of the contract[[11]](#footnote-11). The unique feature of cloud storage, management and regulation poses security and privacy challenges.  Takabi argues that identity formation can no longer be regarded as a given in the post-modern age. It has become a product of self-construction, open to free choice, an obligation which the individual has no choice but to fulfil to the best of his or her ability.[[12]](#footnote-12) The age old "problem of identity" has thus changed its shape and content[[13]](#footnote-13). As a major means of globalisation, online identities are often border-crossing. Traditionally, the identity providers are often foreign companies. Data storage and processing increasingly occurs widely in detached cloud computing. This poses challenges for the current national and international legal systems. The assumption is that activities and identities are focused in the country of residence. When many aspects of everyday life are internationalised they fall under international law which potentially causes challenges. Globalisation did not only increase the options of identification, but has also contributed towards its disintegration. In trying to harmonies online identity, the electronic identity (eID) cards were launched as a new way of digitally recognising the citizens’ identity. The e-identification determines a person’s identity or entity by using electronic means.[[14]](#footnote-14) Palmer rightly states that discourses and struggles of identity have important and far-reaching implications for policy-making on all levels. [[15]](#footnote-15) In Europe 17 member States countries participate in a project called STORK (Secure identity Across Borders Linked) which has proven that e-IDs can be safely recognised across borders. The STORK project promotes mutual recognition of national eIDs, enabling EU-wide citizens to access electronic public services securely in other Member States [[16]](#footnote-16) South Africa has just introduced e-identification system. Gemalto a digital security company based in Netherlands supplied South African Government Printing Works with its Sealys eID cards for national ID card roll-out. The secure embedded software protects the holder’s image and biometric data within the electronic identity document.[[17]](#footnote-17)  The conclusion can be drawn that loss of legislative legs of the stand on globalisation, identity and cloud computing makes it extremely difficult for states to control data. With this in mind the following questions emerge, who owns the data, how is it to be used? Are controls in place? How do we flawlessly integrate legislative frameworks of globalisation, identity and cloud computing internationally? How is risk and regulatory compliance managed when there is no control of infrastructure and data?   1. **THE IMPACT OF AUTOMATED IDENTIFICATION TECHNOLOGIES**   The demand for better methods of identification is growing, driven by the emergence of new technologies that have significantly increased the possibility of creating detailed personal profiles. Automated profiling technologies, for example, use analytic techniques to mine 'big data' – that is, find patterns and correlations in large and multiple databases – to enable the construction and application of personal profiles for commercial, as well as potentially law enforcement and national security, purposes. This technology enables personalised, smart applications and, ultimately, may support ubiquitous computing based on predicted needs and desires. Profiling can involve significant risks. It is often non-transparent in its operation and as to its effects where decisions are taken affecting individuals based on its results. Moreover, profiling mechanisms may lead to erroneous conclusions about a person's identity. Related to profiling is the use of big data analytics in surveillance activities aimed at uncovering hidden behavioural patterns and intentions. For example, surveillance regulation and practices has been drawn into the spotlight in the aftermath of Edward Snowden's revelations about the extent of the US National Security Agency's secret collection and access of communication records and data. These raise questions around how the law negotiates the division between public and private interests where automated technologies are involved.  Possible discussion points include:   * What is automated profiling and how and when can it apply to individuals? * What are the potential impacts of the predictive capacities of profiling techniques on legal concepts such as privacy, due process, proportionality and non-discrimination? For example, fundamental to most legal traditions is the sacrosanct right to be presumed innocent until proven. Yet, the upholding of this principle implies that citizens should not be subjected to intrusive monitoring and data collection until a reasonable suspicion of illegal activity exists. * What legal models are required to address profiling? How can law strike a fair balance between, for example, privacy and security when automated surveillance practices are involved? In particular, how can due process and proportionality be embedded as procedural safeguards into big data profiling technologies aimed at protecting public interests?   **Commentator: Susan Corbett *Associate Professor in Commercial Law, Victoria University of Wellington, New Zealand [Susan.Corbett@vuw.ac.nz]***  *Susan Corbett is based in the Business School at Victoria University of Wellington and teaches an honours course in e-commerce law, commercial law for the MBA, and undergraduate papers in E-commerce law, marketing law, and contract law. Her research is focused on copyright law and digital culture, online privacy law, and cyber-law more generally. She has published widely and presented papers at many international conferences. A selection of recent publications may be viewed at www.victoria.ac.nz/sacl/staff/susan-corbett.aspx . She is currently the legal member of an international research team, funded by the Australian Research Council, which aims to create a playable history of Australasian digital games for industry, community and research purposes. She is a founder member and General Secretary of the newly-formed Asian Pacific Copyright Society (APCA).*  Today, on the internet, everyone knows you’re a dog.[[18]](#footnote-18) The practice of online automated profiling is pervasive throughout the Internet and dispels the commonly-held notion that Internet users are unobserved and anonymous. Since the earliest days of the Internet most websites have automatically collected and stored (in a database) information about a user’s IP address, browser type and referrer. Historically, this kind of quasi-personal information was used to recognise the return visits of a particular user and, in aggregated anonymous form, to allow website administrators to analyse traffic patterns within the website.  Thus, from the time you became an Internet user; your personal information will have been collected and stored by the technology. Furthermore, online data is rarely destroyed, hence your current online ‘profile’ will include historical events from your earlier life, perhaps events you would now wish to conceal, such as a previous bankruptcy or criminal conviction or a long-dissolved relationship.  Moreover, modern technologies can now facilitate the collection, collation and cross-matching databases of personal information about Internet users on a massive scale. This information is not only used to profile the individual user, but also, somewhat more disturbingly, to categorise that individual as belonging within a group profile.  Online profiling is used for many purposes, the main ones being e-commerce (including search engines and social network sites), law enforcement and surveillance. For the e-trader information about the purchasing preferences and lifestyles of their customers is extremely valuable to the business, enabling the business to attract and target users with appropriate advertising and provide the customer with a more personalised service (for example Amazon.com frequently recommends new books to its customers based on their profile; Google “knows” which country you are making your search from). Law enforcers and security agencies have an obvious interest in obtaining information about potential or actual threats to national security.  However for the offline trader or law enforcement agency, the ability to collect personal information and build up a profile of an individual is limited by the nature of the physical environment (individuals must physically provide their information) and the requirement to comply with privacy and data protection laws. Conversely, the virtual nature of the online environment permits personal information to be collected without the individual user’s knowledge or consent. Furthermore the availability of cloud storage facilities means that, for all intents and purposes, there are no practical limits on the quantity of information that can be stored online by a business.  Although privacy laws remain applicable online (albeit more difficult to enforce) and apply to the collection of personal information, the collected data may be subsequently anonymised by data mining technology and therefore will become exempt from most privacy laws. Thus while the collection of the data is in theory subject to privacy regulation, in practice such collection is usually unobtrusive and is therefore unlikely to be subjected to a legal challenge. Once it has been anonymised, the retention of the data and its further use is completely unregulated by privacy laws.  While many would argue that there can be no harm in using anonymised data this belief is, unfortunately, not well-founded. The anonymised data will be used by the technology to create a group profile, which will then be applied to all individuals with certain matching criteria.[[19]](#footnote-19) In this way, for example, an individual might, unknowingly, be blacklisted from being employed in government positions because they happen to have a friend on Facebook who is a religious fundamentalist or who has a serious criminal conviction.  Social networks are another source of personal information that can be used, or misused, for the purposes of online profiling. The personal information that is voluntarily provided when registering with a social network site is usually stated to be kept private by the site administrator. However, the information is used by the administrator to provide functionality within the social network site itself. This use renders the so-called private information vulnerable to attack by potential spammers. Social network sites have been attacked by spammers who provide lists of email addresses which could be ‘friends’ and requesting the social network to put them in touch. In this way the spammer is able to find out which email addresses belong to genuine people and target them with spam.[[20]](#footnote-20)  Finally, a way we can all become online automated profilers! The website, www.whatsyoname.com promises to “search deep within 81 major social networks and find your friends’ secrets - personal photos, videos and more!” The Homepage promises a “people search across social networks, blogs and more”. This service would no doubt shock many of our “friends”. In particular the ability to view an individual’s profile on different social media sites could reveal information that may be highly distressing to the target. For example a user of the business site, LinkedIn, might provide different personal details, such as her age, to LinkedIn from those she provides under a pseudonym to a dating site. The repercussions if this service were to be used by fraudsters or potential employers, law enforcers and other government agencies are very disturbing.   1. **LINKING OFFLINE AND ONLINE IDENTITIES: MOBILE IDENTITY**   The mobile Web is becoming increasingly commonplace as society becomes more hyper-connected due to the rising popularity of smart phones and tablets. Most internet-connecting devices have location-tracking features. These provide opportunities for generating revenues from the provision of location-based services, together with possibilities for effective identity authentication where the location in which a device is used is combined with verification of other identifiers. Thus, there is the potential in the future for online identities to become linked more firmly with the offline domain through the collection of geo-location data. This fact raises significantly challenges to personal privacy and regulation.  Possible discussion points include:   * How can we best manage our digital identities on the move? * As devices are strongly linked to their owners, is identity authentication through hardware the best option? * What options are there to increase location privacy, such as using anonymisation and obfuscation techniques? * Should offline and online identities be linked more firmly as a legal requirement to deter digital identity misuse and abuse?   **Commentator: Nancy J. King *is a Professor of Business Law and Toomey Fellow at Oregon State University's College of Business in Corvallis, Oregon, U.S.A. [Nancy.King@bus.oregonstate.edu]***  *In 2008 Nancy was a Fulbright Fellow at the Centre de Recherches Informatique et Droit (CRID), at the University of Namur in Namur, Belgium. While at the CRID she conducted comparative legal research from an EU/U.S. regulatory perspective on data protection and privacy issues related to consumers' use of mobile phones incorporating location tracking technologies. She has published papers in the American Business Law Journal, Computer Law & Security Review, International Journal of Private Law, Michigan Telecommunications and Technology Law Review and the Federal Communications Law Journal, among others. In 2012 she received the College of Business's graduate teaching award and the Holmes-Cardozo award for her research from the Academy of Legal Studies in Business.*  Discussion of the linking of offline and online identities and the role of mobility raises important questions that go to the heart of what a coherent privacy framework should look like. Now, more than ever before, technology facilitates linking of our offline and online identities, reducing our ability to maintain separate online and offline identities for the purpose of protecting our personal privacy.  The global installation of smart energy meters in our homes to facilitate the societal benefits of the smart grid provides a poignant example that illustrates the implications of having online identities linked to real world identifiers. Linking offline and online identities in this context through the lens of surveillance by smart meters in homes will potentially expose intimate details of people’s personal, family and home lives to outsiders, threating personal privacy/autonomy in a traditionally very private sphere. Along with the introduction of smart meters, more consumers (over 50% in many countries) now have smart phones or other mobile devices with Internet access and location-tracking features that can easily be equipped to give consumers (and others) the ability to remotely access smart meter data. Accessing smart meter data through mobile devices provides convenience for consumers, but it is yet another way that their online and offline identities may be linked, reducing privacy in a traditionally very private sphere.  Additionally, advances in online tracking technologies, including those that enable online tracking without cookies and across mobile devices, make it more difficult for consumers to protect their offline identities. Privacy-enhancing consumer behaviours that have worked in the past, such as using multiple devices to access the Internet (to get a “clean slate” or create multiple online profiles), deleting tracking cookies or using mobile phones (where tracking cookies do not work as well), may no longer be effective. New online tracking methods may use statistical modeling to determine that different devices and computers belong to the same person, enabling marketers and others to know the user’s personal preferences and information no matter which device they use. Further, retailers can read mobile phone identification numbers in offline retail stores and track the consumers’ behaviour without knowing their offline identity. For example, such offline tracking systems are being used by airports in the U.S. to understand passenger behaviour patterns, manage capacity and provide real-time information about the airport. These systems track passengers within the airport by detecting Bluetooth or WiFi signals emitted from smartphones, collecting the phones’ unique device identifier numbers (UDID).  On the other hand, there are technical options to increase location privacy that may help consumers maintain separate offline and online identities in the context of using mobile devices. These include so called “location obfuscation” techniques that may be used in location-based services or information systems to protect the location of the users by slightly altering, substituting or generalizing their location in order to avoid reflecting their real position. However, in some cases, strong arguments can be made for linking offline and online identities as a security protection and/or a legal requirement to deter identity misuse and other harms such as exposure of sensitive personal data. This may be true in the case of providing online and mobile access to sensitive online health information, where potential harms that may result if sensitive personal data is wrongfully exposed may justify requiring patients and their health care providers to verify their offline identities in order to obtain online access to sensitive data.  In sum, the merging of offline and online identities that is now occurring raises important questions about privacy and data protection including whether consumers should have the right to maintain separate offline and online identities, and if so, how this right can be effectively exercised.  **Key References**: Omer Tene & Jules Polonetsky, Privacy in the Age of Big Data, *Stanford Law Review* Online, vol. 64, 63 (Feb. 2, 2012); Claire Cain Miller and Somini Sengupta, Selling Secrets of Phone Users to Advertisers, *The New York Times* (Oct. 5, 2013); Letter, Senator Edward J. Markey to The Honorable Edith Ramirez, Chairwoman, Federal Trade Commission (Oct. 10, 2013); New Offline Tracking Methods Come to Airports, Inside Privacy, at: *www.insideprivacy.com* (Sept. 25, 2013) (posted by Nigel Howard); M. Duckham, L. Kulik and A. Birtley, A Formal Model of Obfuscation and Negotiation for Location Privacy, in *Proc. Pervasive 2005*, LCNC 3468/2005, pp. 243-251 (2005); The Proliferation of Mobile Devices and Apps for Health Care: Promises and Risks, Bloomberg BNA (2013), Nancy J. King and Pernille W. Jessen, “For Privacy’s Sake: Consumer Opt Outs for Smart Meters,” presented at the IAITL 2013 conference in Bangkok, Thailand.   1. **WHAT RESPONSIBILITIES SHOULD INDIVIDUALS HAVE FOR THEIR IDENTITIES? GREATER EMPOWERMENT? GREATER LIABILITY?**   Individuals are looking for ways to increase their levels of control over their data, in addition to opportunities to correct data associated with inaccurate 'portraits' of their identity online. In keeping with this trend, the problem of identity misuse can be portrayed as one that should ultimately rest upon individual responsibility. These facts raise questions around how best to make people more aware of the ways in which value is associated with digital identity, as well as possibilities for making individual more empowered to reap this value and recognise they are liable for the maintenance of their identity data once empowered. Privacy Enhancing Technologies (‘PETs’) are relevant in this context as they help users to disclose their personal data in a controlled and proportionate manner on a ‘needs to know’ only basis.  Possible discussion points include:   * How do you get people to understand that what they put on the Web may stay there indefinitely and can be seen and used in other contexts than those originally intended? * Can we rely upon existing data protection models that aim to give individuals control over their personal data the point of collection, rather than at the point of use? What mechanisms can be used to empower individuals to control how their data is used after it has been collected? * To what extent can identity protection benefit from the principles underlying PETs, i.e. integrating legal protection into the technological infrastructure that can threaten identities? * How can individuals be helped to address inaccurate information about themselves online? Are proposals around data erasure (such as the right for individuals to request that they be ‘forgotten’ by publishers of online content) an effective approach? For examples, how should the law balance the interests of freedom of expression (such as the interests of people to take photos in public places and publish them) versus privacy (such as the interests that people have in protecting their image where it is taken and used without their consent)? * What is the best way to deal with protecting anonymity on the Web? Is reliance on data anonymity and pseudonymity techniques to protect identities overrated in light of the ever-expanding capacities for advancing technologies to blur the distinction between attributable identity (where an identity can be attributed to a physical person) and unattributable identity (where such attribution is not possible)? Should an unattributable identity be treated as ‘personal data’ under data protection law?   **Commentator: Kah Leng Ter *LL.M (Bristol); Barrister (Lincoln’s Inn); Advocate & Solicitor (Singapore); Associate Professor at the NUS Business School, National University of Singapore [bizterkl@nus.edu.sg]***  *Kah Leng Ter has been a Visiting Scholar at McGill University and the Universities of British Columbia, London and recently, Sydney. Her research interests include IT law, commercial contracts and data protection. She publishes regularly in these areas.*  Individuals are constantly disclosing personal identifiable information (PII) when they communicate over the Internet, enter into web transactions or share personal information through social media. PII that is traded online has great commercial value but it is extremely sensitive information that needs to be strongly protected. A most significant concern is the risk of online identity theft and fraud. Identity theft has been described as “the fastest growing crime of the 21st century” that can result in loss of credit rating and reputation.  Since individuals have control over the level of PII that they share, the disclosure and protection of their own identity data online should ultimately rest upon personal responsibility. However, individuals should not be held solely responsible. Under data protection legislation, such as the Singapore Personal Data Protection Act of 2012, organisations are responsible for the personal data that they collect, use or disclose and must make security arrangements to protect such data. Among other measures, they are expected to have a data privacy policy in place, educate pro-actively on good security practices, provide secure sites with encrypted web pages and provide support services to help customers. A pro-active approach enhances consumer trust and confidence and builds trust in brands. Thus, service providers can no longer say that individuals have control over what they share publicly and abdicate responsibility. As the recent Experian Consumer Identity Risk Report of 2013 shows, 47% of UK internet users in the survey believe it is their personal responsibility to protect their own identity online while 40% of the respondents place the responsibility on the providers of online services. 4% look to the Government while the rest are undecided.  How can individuals discharge their responsibility for their PII? Both technology and legislation provide empowerment opportunities for individuals to have greater control over their identity data. There are best practice security measures such as using strong passwords or different passwords for multiple accounts, avoiding questionable websites and not falling victim to online scams. There is also security software including identification protection products which provide support against identity theft and the services needed to address the problem quickly. The CPP Group, a pioneer in the Life Assistance market, in partnership with the Credit Bureau of Singapore, offers credit reports and alerts that will quickly identify and notify individuals of any unusual financial behaviour so that they can take the necessary protective measures. Online anonymity and pseudonymity may be a good way to protect identities of data subjects, but law enforcement officers fear that this will be used by criminals to disguise their identities. Perhaps the future of anonymity will depend on identity management infrastructure that ties online identity to a person’s legal identity. Under such an identity system, users are required to sign in using legal names.  Data Protection legislation also gives empowerment in the form of the following rights: consent, access and correction, not to have data kept longer than is necessary, the right to disappear and to stop PII from being used in direct marketing, data sharing and trade, pursuant to a Do Not Call Registry. These rights empower individuals to control how their data is used or disclosed after it has been collected.  A final issue is the consequences of identity theft. In the case of stolen identity resulting in online banking fraud, on which party should the consequences fall? The position in Singapore is generally governed by the terms and conditions between the bank and customer. The customer is required to notify the bank immediately if his/her Card is stolen or if the PIN has been compromised. Once the bank establishes that the loss or theft of the Card or PIN compromise was not caused by the customer’s fault or negligence, the customer’s liability for unauthorised transactions carried out after such loss, theft or unauthorised disclosure but before the bank is notified is capped at S$100. The customer will not be liable for any transactions carried out after the customer has notified the bank. The bank will refund the amounts deducted from the bank account for unauthorised transactions, in excess of the applicable liability cap, within 14 working days from the time the customer submits all the necessary information to the bank.  With regard to criminal responsibility for identity theft, the Singapore Computer Misuse and Cybersecurity Act provides that any person who accesses computer data with intent to commit fraud or dishonesty, shall be liable to a fine not exceeding S$50,000 or imprisonment not exceeding 10 years or to both. The Act has extra-territorial reach as it applies to offences committed outside Singapore as if they were committed within Singapore. However, enforcement problems are envisaged due to the proviso that the accused must be in Singapore at the material time or the computer, programme or data was in Singapore at the material time. Furthermore, as these are criminal proceedings, the victim will only be compensated if the person liable is ordered to pay civil compensation for damage caused to the computer, programme or data.   1. **TRENDS IN PERSONAL IDENTIFICATION: FROM TOKENS TO BODY SURVEILLANCE**   Proving one’s identity has relied for many years upon the possession of physical tokens, such as identity cards. Yet biometric technologies, such as fingerprints and iris scans, are becoming more widely used in everyday life due to the inherent link between them and the physical person whose identity is being authenticated. Tying identity assurance functionality to devices using biometrics is a new trend, typified by the recent inclusion of a fingerprint log-in sensor on the iPhone 5S. Recognition of physical behavioural patterns may also grow to be a key element in the verification of people with monitoring systems that draw behavioural profiles of users. In effect, our digital identity will encompass a physical part of us that can be launched into the online world, as well as being applied forensically in the criminal justice system. Digital imaging technologies acquire and process biometric images of increasingly high quality. However, some biometric technologies, such as automatic facial recognition, are still sometimes found to be insufficiently robust evidence in court. Furthermore, direct technological links between people and digital networks using sensors that can transmit biological data bring the very notion of what it is to be human into question raising ethical and legal dilemmas.  Possible discussion points include:   * Since technology is rapidly advancing in this area, how do we update laws and regulations in order to protect fundamental human rights and what types of laws and regulations would work best? * How do we strengthen the data protection principle of informed and explicit consent in relation to the automatic collection of biometric data? * How do we distinguish and define biometrics deemed sufficiently worthy of legal protection? * Do we need specific data protection rules regarding DNA data because of the information that can be elicited surreptitiously from it, such as in relation to family relations of the data subject? * If sensitive biometric data is stolen, what type of proof will be required in the future for its owner to escape liability for the effects of its fraudulent misuse? |
|  |

**Commentator: Alison Knight**, ***Solicitor and Researcher at the University of Southampton; www.southampton.ac.uk/ilaws/teaching/alison\_knight.page [A.M.Knight@soton.ac.uk]***

*I qualified as a lawyer in 2001, working for several years for a law firm in London and Brussels where I specialised in Competition Law and European Commission investigations. I returned to the UK in 2004 joining the Government Legal Service. More recently, I worked for a number of years for a large, commercial law firm where I developed my interest in Information Communication and Technology legal issues. In 2010, I completed an LLM including Internet Law, followed by an MSc in Web Science, with the University of Southampton. Currently, I am completing a PhD around digital identity and legal issues with Southampton Law School and its Institute for Law and the Web. I am also a member of the Web Science Doctoral Training Centre at the University of Southampton, which is part of a £250 million investment in the future of UK science and technology by the RCUK Digital Economy Programme. Alongside my PhD, I give legal advice to the multidisciplinary Super Identity research project, the wider objective of which is to work towards a rich understanding of identity that encompasses aspects that we reveal both in the real world and in the cyber world.*

Identification is critical in our networked world. Society needs reliable and effective methods to establish the identity of unknown individuals and authenticate existing identity credentials for both public and private ends. Governments, in particular, are under pressure to implement policies that take advantage of the latest tools for identification of their citizens in keeping pace with increasing concerns about online identity theft and national security. Yet means of identification vary depending upon the purpose for which identification is required. Different periods of history and cultural preferences also favour different approaches.

The introduction of trusted identity credentials in the form of physical tokens relied originally upon the assumption that the individual who possesses a token is its proper owner. An example is a state-issued birth certificate deemed to confirm the identity of the bearer asserting to share the same name and date of birth on the paper record. Increasingly in the 20th Century, paper-based examples incorporated physical identifiers (such as photos in passports), which could be subject to face-to-face human verification. More recently, the electronic environment has introduced a shift-change in identification capabilities. The incorporation of digital features, such as computer chips, into physical tokens enables more secure authentication. There has also been a shift towards knowledge-based schemes, such as a password or personal identification number to validate identity offline and online.

Although possession of physical tokens or informational knowledge suggests that they been provided to or chosen by us, neither, however, connects intrinsically to us. Moreover, both modes are vulnerable to forgery and misappropriation. Consequently, new identification techniques have developed that take advantage of rapid technological developments in body surveillance. Lyon describes this trend as the “co-opting of the body itself as a means of identification”. [[21]](#footnote-21) A notable example is automated biometric technology that uses software to compare samples of physical characteristics (such as a fingerprint or iris) from a person against raw biometric templates to confirm their identity.[[22]](#footnote-22)

Biometrics is used increasingly in everyday life due to the strength of the link between them and the physical person whose identity is being authenticated. The value of a biometric is enhanced when it carries unique or near-unique characteristics that are stable and resistant to change. Such biometric traits are a preferred security standard as they are inherent to the individual and cannot be lost or transferred. Some show strong anti-spoofing capabilities and others require evidence of viability of life making them difficult to use fraudulently.

Biometric technologies are popular with governments for population monitoring, such as in border control procedures. They are also used in commercial applications. Concerns loom large, however, about their legal and social acceptability. As biometric technologies have the potential to erode individual privacy, a minimal data disclosure principle is recommended. How much and what type of biometric data can be required legitimately by identity assurance schemes to operate, for example, is however open to debate. Furthermore, identification information in the form of sensitive biometrics data may be extracted from the body without the consent of those people subject to the technology. Notable examples include automated facial recognition technology.[[23]](#footnote-23)

Other noteworthy concerns include the fact that our biometric samples (our ‘digital extensions of physical self’) may still be liable to tampering or impersonation, with great risk to the individual if misappropriation takes place that compromises future use of that biometric. This risk intensifies as biometric data circulates increasingly online. In addition, the security offered by biometric technologies is not failsafe leading to the possibility of wrong identification. There are dangers that scientific rigour may be traded away for intelligence gathering and surveillance purposes, ultimately to the detriment of individuals.

Biometric technologies can also recognise the expression of people’s behavioural traits (such as their gait or keyboard strokes) enabling remote identity verification. While such biometrics is unlikely to carry unique identifiers, they “may be expected to offer sufficient discriminatory information to permit identity verification”.[[24]](#footnote-24) Body surveillance technologies also encompass location-tracking tools attached to tokens or devices. With GPSes increasingly being installed in our cars, alongside smartphone in our pockets, the potential for privacy intrusion (particularly by corporate giants) grows as does the future prospect of implanting radio-frequency identification (‘RFID’) chips directly into the human body.

Thus, while technology can exploit our physical distinctiveness to identify us thereby reducing identity deception and enhancing security and efficiency, body surveillance can also be privacy’s foe and raise legal and ethical concerns. The body has become “a source as well as a site of surveillance… [that] can be directly scrutinized and interrogated”.[[25]](#footnote-25) The risks increase if body surveillance technologies become widespread with the likely permeation of multi-sensory biometric systems and automated observation in our everyday lives, much of which may apply unobtrusively without the knowledge and/or consent of individuals. Even the threat of surveillance can affect the behaviour of those who feel that they are under blanket suspicion of having something to hide.

Whether being identifiable by something you are, as opposed to something you possess or know, is preferable, therefore, depends on a careful balancing of trade-offs between security, convenience and privacy risks. In carrying out this analysis, policy makers should be careful not to see body surveillance technologies as an automatic panacea for all societal problems associated with identification without evaluating carefully the broader implications. In particular, lawmakers must face up to the possibility now that in the future our “data doubles”[[26]](#footnote-26) may become our primary means of identification and the dangers this might hold for individuals and their legal rights.

**9. THE PUBLIC DEBATE ON THE PROCESS OF CREATING A BIOMETRIC DATABASE**

Concerns are high about the privacy implications of collecting and using biometric data, as well as its storage in government-controlled databases. Concerns revolve particularly around the possibility of ‘function creep’: that biometric data collected for one legitimate purpose may, unbeknownst to the individual from whom they were extracted, later be used for other illegitimate ones. More widely, there are societal questions raised regarding the risks inherent to the existence of a vast and sensitive database resource, which creates unprecedented opportunities for a state to monitor its citizens.

Possible discussion points include:

* What rules are required in order to prevent inappropriate processing, sharing and trading of biometric data?
* How do we ensure more transparency regarding the purposes for which biometrics might be used, together with any associated risks to the individual?

**9.1. THE PUBLIC DEBATE ON THE PROCESS OF CREATING A BIOMETRIC DATABASE IN ISRAEL**

**Commentator: Dr. Tamar Gidron *(LLB, Hebrew University, Law Faculty Jerusalem. Israel; LLM and Dr. Jur.: Tel-Aviv University Law Faculty Israel) [tgidron@netvision.net.il]***

*Tamar Gidron 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*

**Commentator: 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@gmail.com]***

*Uri Volovelsky is an associate at Caspi & Co. one of the oldest law firms in Israel. He primarily works in the Corporate and Mergers and Acquisitions department. His position involves representing Israeli law firms in a variety of business transactions with foreign corporations including, inter alia, mergers and acquisitions. In addition to his practice as a lawyer, Uri Volovelsky holds a position as a researcher and teaching assistant in the fields of corporation law, defamation, torts, commercial contracts and instruments of payments at the College of Management Academic Studies. His thesis was entitled: "Judicial Intervention in International Arbitration – Comparative Analysis Israel, England, the United States and France".*

Even though the cataloguing of fingerprints is attributed to Juan Vucetich back in 1891,[[27]](#footnote-27) in recent years we have witnessed a growth in the cross-border worldwide debate over the use of biometric information (such as facial features and fingerprints) for the purpose of identifying individuals for security reasons and access control. Two separate but yet connected questions arise with respect to the use of biometric information. First, whether biometric information should initially be collected. Second, assuming that the answer to the first question is affirmative, whether there is a genuine need that the information will be collected in a designated database. The debate which raises important substantial – practical alongside ethical questions – was (and shall continue to be) the subject for extensive writing. The purpose of the below brief but yet comprehensive discussion is twofold. We begin with presenting the proposed legislation in Israel for the collection and use of biometric information by the Israeli government. In continue with a comparative examination of the type of solutions other countries have adopted with respect to the collection and use of biometric information. We reach the conclusion that the proposed Israeli solution is a unique experiment compared to other member’s states of the Organization for Economic Co-Operation and Development (“**OECD**”).

For many years, indeed since 2007, the Israeli Ministry of the Interior has been pursuing a plan to issue “smart” identity cards containing microchips that cannot be forged.

The trigger for the proposal was a wave of counterfeited identity cards as well as internal and foreign security concerns that in Israel have an important impact on legislative considerations.

In 2009 it was decided that the data accumulated in the process of issuing the new ID cards would be kept in a database holding the biometric information of all the residents of the country.

The decision to add to the issue of smart documentation the establishment of a biometric database sparked a fierce debate both within and outside public administration: elected officials, well-known scientists, academics, information security experts and ordinary citizens warned against setting up the database and demanded that only smart cards be used.

In view of these objections, a compromise was achieved whereby the existence and operation of the database would be made contingent upon the results of a “pilot scheme”, which would be managed in accordance with an official statutory instrument and supervised by public measures, which would examine the necessity of the database, the scope of the information stored in it and how it would be used.

The Knesset only passed the bill after it was amended in accordance with the above compromise.

The Israeli Civil Rights Movement, supported by internationally renowned professors, has petitioned the Supreme Court of Israel to halt the establishment of the database (they do not object to the issue of biometric cards) and they, together with other activists who fear the violation of the right to privacy, are conducting a very strong campaign against the Law.

The principal objections are that the general public database is a vast and sensitive information resource, and creates an unprecedented mechanism for monitoring and control. It causes severe and unnecessary harm to human dignity, freedom and the right to privacy. It undermines the foundations of democracy and, in addition, is a danger to public peace and safety.

Arguments have also been made against the legitimacy of linking the legitimate goal of upgrading the Israeli ID cards to the establishment of the database. It is contended that a central biometric database is not needed, nor is it intended to prevent the falsification of identification documents. To do so, it would be sufficient to issue certificates with a microchip (similar to credit cards) in which biometric or other data is embedded.

Even after the introduction of the database, a person's identity would continue to be verified by comparing the data contained in the card displayed by the person against other means of identification produced by him: PIN code, fingerprint or other means of identification.

In contrast, a biometric database such as that planned in Israel, would be used primarily to identify people; using a computer check, a fingerprint or facial photograph of an unidentified man would be compared to the biometric data of the entire population, stored in the database.

Prima facie, the debate regarding the biometric database is a reflection of the conflict between the individual’s right to privacy and the collective interest in security, even though there are many who emphasize the public nature of the interest protected by the right to privacy.[[28]](#footnote-28) This conflict does not lead to unequivocal black or white results; rather it is an argument where there is support for each of the two opposing opinions.

Alongside the factual debate between supporters and opponents of the database about whether similar databases already exist in the world and the experience which has been garnered in respect of them,[[29]](#footnote-29) issues of principle have also been enlisted to justify the fight against the database, such as the possibility – some say certainty – that the database will be hacked and that the resulting harm will be much greater, that the ability to engage in impersonation, identity theft and other fraud will become much more sophisticated, and in particular that the database is unnecessary and consequently the danger that it creates is unacceptable. It is also claimed that the law violates fundamental rights protected by the Basic Laws of Israel to a disproportionate extent.[[30]](#footnote-30)

Despite massive efforts of persuasion, currently, Israelis are voting with their feet and the response to the temptation offered by upgraded certificates is quite low.

Against this background, the following brief comparative survey is interesting:

The attack against the World Trade Center in New York on 9/11 marked the “opening shot” in the aspiration of governments to establish biometric databases as a means of securing borders, control immigration into the country, convict criminal suspects, prevent identity theft and pursue counter-terrorism. The public and legal debate in various countries regarding the use of biometric information focuses on two issues – the first issue concerns the question whether issuing biometric identity cards and/or passports is necessary (cost v. benefit). Based on the assumption that the answer to this first question is affirmative, one may ask whether it is necessary to store the biometric information in a special database.

The global trend today among the member states of the OECD (apart from specific exceptions such as Mexico) is to withdraw from the plan to establish biometric databases. Even countries which have taken initial steps to establish a biometric database have retreated from these intentions following public opposition. Below are some examples:

**\* Netherlands** – In 2009, obtaining an ID card was made contingent upon the provision of fingerprints. The collection and storage of biometric information was performed in accordance with the Personal Data Protection Act, 2011. In 2011, the collection and storage of biometric information was suspended in light of invasion of privacy concerns. The use of biometric identity cards was also suspended in light of questions about the reliability of biometric information, particularly in relation to the ability of existing technologies to reliably identify the holders of a biometric passport or ID card. However, in 2012 a bill was introduced whereby immigrants applying for visas to the Netherlands were required to provide their fingerprints and passport photos for storage in a biometric database.

**\* France** - In 2012 a law was enacted providing that citizens of France be issued with identity cards and passports that would include biometric information (including facial features, fingerprints and eye colour). The biometric information would be embedded in a chip on the ID card. In addition, according to the bill, there would be a voluntary option whereby the identity card would include an additional chip allowing the execution of an electronic signature for the purpose of e-government services and e-commerce. The Conseil Constitutionnel (France Constitutional Court) stated that the establishment of a biometric database was contrary to the fundamental rights guaranteed by the French Constitution, including the right to privacy and the presumption of innocence.

The French court held:

*“The collection, registration, preservation, consultation and communication of personal data have to be justified by a general interest reason and carried out properly and proportionally"… "Regarding the nature of the recorded data, the range of the treatment, the technical characteristics and conditions of the consultation, the provisions of article [...] touch upon the right to privacy in a way that cannot be considered as proportional to the intended purpose."*

The stated objectives of the Law were "preventing identity theft". Nonetheless, in practice, the law would also have allowed the use of databases for security and judicial purposes. This course of action was rejected by the Court. Regarding the commercial benefits that were expected to ensue from the use of certificates that include biometric information, the Court ruled that no proportionality existed between the benefit to be gained from the use of the database and the absence of adequate protection mechanisms for guaranteeing confidentiality.

**\* England** – The English position is a far-reaching example of the use of biometric databases. The initiative of the British government was to issue biometric identity cards which would include a chip containing a link to a concentrated biometric database that would include information on all the residents of England classified according to no less than 50 categories. According to the initiative, there would be a duty to update the information on a regular basis and a record would be made every time the information was updated. This initiative was attacked by its opponents on the ground that the collection, maintenance and duty to update the information would lead to “life-long surveillance" and consequently to infringement of privacy and violation of the concept of life in a free society. Despite 10,000 biometric ID cards being issued, the Law was repealed at the behest of the elected government and the ID cards were declared to be invalid.

**\* Germany** – no biometric information is stored in designated databases. At the same time, obtaining an ID card is made contingent upon the provision of fingerprints.

In order to provide a complete and accurate description of EU law regarding the collection and storage of biometric information, two important case law decisions should be briefly mentioned.

The European Court of Justice (“**ECJ**”) was asked by Netherlands and Germany states courts to rule whether local states legislation empowering local authorities the right to decline citizen’s request for passports who refuse to supply their fingerprints contradicts European Union (EU) Charter and the European Convention of Human Rights (“**ECHR**”). The ECJ ruled that that national legislation of EU Member’s States requiring the provision of fingerprints as a condition for obtaining a passport is lawful and does not violate the basic right to privacy, entrenched in the European Union (EU) Charter and the ECHR.[[31]](#footnote-31) However, the court clarified that the fingerprints may be used only for the limited purpose of verifying the authenticity of the passport and the indemnity of the passport holders. The Court also specifically stated that the storage of the fingerprints may only be done within the passport itself, which belongs to the passport holder and not part of a designated database.

It is also important to mention the ruling given by the European Court of Human Rights regarding privacy and biometric information in the case *of S. and Marper v. The United Kingdom*.[[32]](#footnote-32) The case involved the collection of fingerprints and testing of DNA during the arrest of suspects. Following the suspects release, the police refused to destroy the information despite a direct request. The Court held that the long-term retention of fingerprints and DNA samples violated the right to privacy and therefore constituted a breach of Section 8 of the ECHR. As we can see the Israeli experience is but one in the chain of attempts to establish a central biometric database by means of issuing biometric identity cards /passports. The fate of the Israeli process remains unclear.

1. http://www.intel.com/content/www/us/en/communications/internet-minute-infographic.html Date of access 21/10/2013 [↑](#footnote-ref-1)
2. http://www.oecd.org/sti/ieconomy/49338380.pdf Date of access 21/10/2013 [↑](#footnote-ref-2)
3. Adopted from my paper “Protecting Privacy and Control of Online Personal Information” and another paper with Budeli ‘Globalisation: “A Nightmare for the Working Class”? for the conference. [↑](#footnote-ref-3)
4. Some authors deny the existence of globalisation and those who accept its existence disagree on whether it is a completely new phenomenon or has existed for a long time. See Kaufmann C (2007) *Globalisation and Labour Rights* at 6.See also www.imf.org/external/np/exr/ib/2008/053008.htm (accessed on 08/08/2010). Schmidt *Trade Union responses to Globalization: A review by the Global Union Research Network* Geneva, International Labour Office, 2007, at 8. [↑](#footnote-ref-4)
5. Cooper F., “What is the concept of globalisation good for? An African Historian’s Perspective” *African Affairs* (2001) 189-213 at 196. [↑](#footnote-ref-5)
6. Hermans J.M Hubert and Dimaggio Giancarlo,  *Self, Identity, and Globalisation in Times of Uncertainty: A Dialogical Analysis*, Review of General Psychology 2007, Vol 11, No. 1, 31-61 [↑](#footnote-ref-6)
7. Palmer G. Tom,  *Globalisation, Cosmopolitanism and Personal Identity* Etica & Politica / Ethics & Politics, 2003, 2 http://www.units.it/etica/2003\_2/PALMER.htm accessed on 25 October 2013. [↑](#footnote-ref-7)
8. Takabi, H. and Joshi J.B.D. (2012) ‘Semantic-based policy management for cloud computing environments’ *Int. J. Cloud Computing*. Vol.1. Nos2/3, pp119-144. [↑](#footnote-ref-8)
9. *Ibid.* [↑](#footnote-ref-9)
10. *Ibid*. [↑](#footnote-ref-10)
11. *Ibid* [↑](#footnote-ref-11)
12. Takabi, H. and Joshi J.B.D. (2012) ‘Semantic-based policy management for cloud computing environments’ *Int. J. Cloud Computing*. Vol.1. Nos2/3, pp119-144. [↑](#footnote-ref-12)
13. *ibid* [↑](#footnote-ref-13)
14. Bornman Elirea “*Struggles of identity in the age of globalisation*” *COMMUNICATIO* Volume 29 (1 & 2) 2003. [↑](#footnote-ref-14)
15. Bornman Elirea, ‘*Struggles of Identity in the Age of Globalisation: Searching for Anchors that Hold’* University of South Africa Department **of** Communication Science, University **of** South Africa. http://www.unisa.ac.za/contents/faculties/humanities/comm/docs/Struggles of identity in the age of globalisation.rtf accessed on 25 October 2013. [↑](#footnote-ref-15)
16. http://www.eid-stork.eu/ accessed 25 October 2013. [↑](#footnote-ref-16)
17. # New SA ID cards: stopping frauds and copies,

    http://mybroadband.co.za/news/government/80625-new-sa-id-cards-stopping-frauds-and-copies.html [↑](#footnote-ref-17)
18. The title of this piece refers to the comment by the computer-savvy dog in Peter Steiner’s famous cartoon, “On the Internet, Nobody Knows You’re a Dog”, (July 5, 1993) *The New Yorker*. [↑](#footnote-ref-18)
19. See further W Schreurs, M Hildebrandt, E Kindt and M Vanfleteren, “*Cogitas, Ergo Sum*. The Role of Data Protection Law and Non-Discrimination Law in Group Profiling in the Private Sector” in M Hildebrandt and S Gutwirth (Eds) *Profiling the European Citizen*, Springer Science Business Media B.V. 2008, ch 13. [↑](#footnote-ref-19)
20. See M Balduzzi, C Platzer, T Holz, E Kirda, D Balzarotti and C Kruegel, “Abusing Social Networks for Automated User Profiling”, Eurecom Research Report RR-10-233- March3, 2010. [↑](#footnote-ref-20)
21. Lyon, D. (2001). Under my skin: from identification papers to body surveillance. In: *Documenting individual identity: The development of state practices in the modern world*, 1, 291-310. [↑](#footnote-ref-21)
22. Biometric technologies are “automated methods of verifying or recognizing the identity of a living person based on a physiological or behavioural characteristic”. Wayman, J. L. et al (Eds.). (2005). *Biometric systems: technology, design and performance evaluation*. Springer. [↑](#footnote-ref-22)
23. See, for example, recent news that a leading UK supermarket plans to introduce facial recognition systems into its stores: http://www.theguardian.com/business/2013/nov/03/privacy-tesco-scan-customers-faces. [↑](#footnote-ref-23)
24. Monrose, F., & Rubin, A. (1997). Authentication via keystroke dynamics. In *Proceedings of the 4th ACM conference on Computer and communications security* (48-56). [↑](#footnote-ref-24)
25. Lyon, D. (2001). Under my skin: from identification papers to body surveillance. In: *Documenting individual identity: The development of state practices in the modern world*, 1, 291-310, p.291. [↑](#footnote-ref-25)
26. Walby, K. (2005). Open-street camera surveillance and governance in Canada. *Canadian Journal of Criminology and Criminal Justice/La Revue canadienne de criminologie et de justice pénale*, *47*(4), 655-684. [↑](#footnote-ref-26)
27. U.S. National Library of Medicine, https://www.google.co.il/#q=Juan+Vucetich+. [↑](#footnote-ref-27)
28. Paul Bernal, *Individual Privacy vs Collective Security? NO!,* Inforrm’s Blog – The International Forum for Responsible Media Blog (Oct. 20, 2013) http://inforrm.wordpress.com/2013/10/20/individual-privacy-vs-collective-security-no-paul. [↑](#footnote-ref-28)
29. Margaret Hu, *Biometric ID Cyber surveillance*, 88 Indiana L.J. 1475 (2013). [↑](#footnote-ref-29)
30. Omer Tene, *Law* 17(2) 1983, 4 – 421. [↑](#footnote-ref-30)
31. *Schwarz v. Bochum*,  [2013] EUECJ C-291/12, [2013] WLR(D) 386. [↑](#footnote-ref-31)
32. *S. & Marper v. The United Kingdom*, [2008] ECHR 1581. [↑](#footnote-ref-32)