Digital privacy in a media orientated world

Rolf H. Weber* and Dominic Staiger

Faculty of Law,
University of Zurich,
Switzerland
Email: rolf.weber@rwi.uzh.ch
Email: dominic.staiger@rwi.uzh.ch
*Corresponding author

Abstract: The article introduces the key challenges in a media oriented world focusing on the surveillance capabilities as well as potential risk mitigating strategies. Furthermore, the key legal provisions governing media devices in the US, the EU as well as Australia are assessed.

Keywords: surveillance; media; privacy; data protection.

Reference to this paper should be made as follows: Weber, R.H. and Staiger, D. (2017) 'Digital privacy in a media orientated world', *Int. J. Public Law and Policy*, Vol. 6, No. 1, pp.21–38.

Biographical notes: Rolf H. Weber is the Co-Director of the European Law Institute, the Center for Information Technology, Society and Law and the University Priority Research Program "Financial Market Regulation" at the University of Zurich. From 2008 to 2015, he was a member of the Steering Committee of the Global Internet Governance Academic Network (GigaNet) and European Dialogue on Internet Governance (EuroDIG) and since 2009, he is a member of the High-level Panel of Advisers of the Global Alliance for Information and Communication Technologies and Development (GAID). His core areas of research include financial market law as well as IT and privacy law.

Dominic N. Staiger is a Researcher at the Center for Information Technology, Society and Law at the University of Zurich. His areas of specialisation includes data protection and IT law with a particular focus on emerging technologies.

1 Introduction

1.1 Information age

Over the last decade the utility of digital media has exponentially increased through the remote provision of services facilitated by cloud computing and widespread broadband access. Today, people use a wide range of media devices and software to communicate as well as to organise and simplify their lives. These technologies collect and retain vast amounts of data which reflect the core of our being. Traditional forms of media (TV, newspapers) that are commonly defined as a communication channel through which data

or information is disseminated[1] are losing ground in light of cloud computing, social media, and other innovative services.

Fitness and health data is collected today by wearables (i.e., Fitbit) thus allowing users to determine how their health has progressed over time and to adjust their eating habits accordingly with the support of an App that monitors their diet. This information is communicated to the cloud which allows users to compare their data to that of other people in their age group. Furthermore, mobile phones constantly monitor the location and movement of their owners and send the data to social media services such as e.g. Facebook which can then inform friends of their location or suggest services in their vicinity.

In addition to these more general monitoring capabilities commercial technologies have emerged that allow tracking and monitoring of people's behaviour in an unprecedented fashion. These technologies require proactive measures to limit their effectiveness and impact on the individual. Furthermore, media use in various age groups must be analysed and privacy risks addressed. Often the amount of data shared as well as the risks associated with the distribution of information is not understood due to a lack of education on how the most common technologies work.

Technology and media are steadily influencing the extent to which we can form and alter our own identity. Already in 2002 the Australian Privacy Commissioner highlighted:

> "Identification is the action of being identified, of linking specific information with a particular person. An individual's identity has a degree of fluidity and is likely to change over time. The extensive linking of different information about an individual may restrict or limit this fluidity".[2]

The rise in data collection allows various forms of monitoring and identification and presents unique challenges for identity protection not only for journalists or other people with an increased need to keep their identity or their communication secret but also for the average media user. In order to reduce privacy risks these people should minimise their digital footprint by not participating in social media postings, avoid tagging and uploading pictures into the digital world, utilise encrypted Email programs[3] for their communications as well as employ secure login technologies such as tokens which are hard to decrypt. However, doing so will invariably attract the suspicion of law enforcement or surveillance agencies in particular when a person of interest such as an investigative journalist is taking such measures to keep his contacts and communication private.

1.2 Sharing pictures and videos

Sharing photos and videos has become part of many people's daily routine. This media data is either stored in the cloud or on the devices themselves. At the time of taking a photo or video the data is also tagged with the geolocation of the device, thus it contains information where and when the photo was taken. Additional information about when and where the data is uploaded is also stored by the social media websites such as Facebook, Instagram or Twitter. As this type of data is very personal in nature and often portrays people or personal connections it must be closely analysed; this analysis has to include the fact that not only the information is supplied to these sites but also that the rights to use the data granted to these enterprises through their terms of service are exercised within a clear legal framework.

Facial recognition software used by Facebook and other media services allow these companies to connect people with each other and establish a comprehensive overview of a person's social network and connections. This data can then also be used for targeted advertisements, sold to other data collectors or supplied to government agencies which add it to their pool of Big Data allowing pattern recognition. The accumulation of data to Big Data allows a vast amount of analysis enabling the identification of individuals and their behaviour. Thus, the user of a media service is not aware for what purposes his data is being used and has only limited means of preventing the disclosure to government agencies which may be located in other countries.

2 Forms of data collection and surveillance risks

2.1 Mobile phone identification

Smartphones contain a number of identifiers that can be used for a wide range of purposes. Every handset has a hardware identification number, a so called IMEI (International Mobile Equipment Identity). This number allows the network operator to identify a personal device even despite potentially different sim cards being used.

Apps which are the backbone of every smart phone can either be supplied through an App store (Android or Apple) or through a third party vendor. Every time an App is downloaded from an App-store information as to what Apps are installed and used on a device are sent to the provider. Thus, this information, although beneficial for keeping the Apps up to date, allows the provider to gain an insight into the user's interest by simply looking at the App list. Furthermore, App browsing and other App use is monitored through some form of ID such as Apple IFA (identifier for advertisers) or Google Android ID.

2.2 Browser tracking

Most people are aware of the fact that browsers record the history of sites visited for a certain period of time but this function can be easily disabled in the browser settings. More sophisticated tracking technologies such as cookies have been installed on most websites. They record the IP address of the visiting computer as well as what sites it opens and for how long. Any searches conducted are also recorded. These cookies can be blocked through appropriate software and browser settings. Thus, the industry has developed new measures for the identification of a computer which are far more difficult to prevent, for example browser fingerprinting that does not require any form of software installation such as a cookie as it only uses the browser settings for identification.

When a browser wants to open a website it first checks whether it supports all the styles and plugins required. In order to do this it sends data in its own configuration to match it with the host's requirements. In doing so it provides the website with a unique fingerprint. The likelihood of two browsers being the same is negligible based on the vast amounts of settings available. In this scenario the browser data is used to identify the device through its unique combination of settings such as display resolution, language, fonts and other data. Studies have shown that with this method 94% of browsers can be identified and effectively linked to a user.[4]

However, changes in the browser or device constellation may alter the digital fingerprint. Although this appears to mitigate the tracking risks, a simple algorithm is able to predict changes with over 99% accuracy.[5] Thus, browser fingerprinting is very effective as it cannot be easily detected because it does not leave any persistent evidence on the computer. Information that is transmitted from the user's browser is sufficient to find out for example whether a flash plugin is installed or whether a list of fonts is supplied. If this list is not present it can be inferred that a flash blocker is installed on the browser.

Once a unique browser fingerprint is generated the device can be identified globally. Only a substantial change in the browser configuration will break this identification capability. When the fingerprint carries more than 15-20 bits of identifying information the browser can be identified in combination with its IP address.

Web beacons are also widely used in order to track a computer. These beacons consist of miniature pictures in the size of only one pixel which cannot be seen by the eye and enable companies to determine whether the user has accessed certain content. The only way to limit the amount of information that is being collected is to turn off cookies and install anonymity plugins or to use a Tor system which routes the data through various gateways obscuring a person's identity.

Ghostery is a browser extension that can identify various tracking technologies and block them.[6] However, the company producing Ghostery has also been subject to scrutiny as once the user has opted-in to a so called Ghostrank option (a tool to improve performance) the user data will be supplied to enterprises with the aim to improve customer experience. Ghostery strongly points out that it will not share data with advertisers to directly market products to consumers.

Furthermore, most free Virtual Private Network (VPN) providers use the information they gain through the data transmission process for their own commercial benefit. As all of a user's traffic flows through its servers the VPN provider knows everything, starting with the websites visited, who and when the user is emailing, how long and when the user is online, the location and what applications the user is utilising. This private information is highly valuable for advertising companies which aim at targeting their ads to a specific target group. Thus, major technology companies such as Microsoft are expanding their influence by buying providers in order to carry out deep analytics of their users to specifically target them with products and services as well as gain insights into how people use their smartphones. The user often is not even aware who owns the company nor has he/she read the privacy policy which allows for such actions. This policy includes measures such as abolishing the privacy of IP addresses.[7] Even free firewalls and antivirus programmes present a threat to individual privacy as these programs are also capable of spying on browser history.[8]

2.3 Electronic payment systems

Credit cards as well as other electronic payment methods such as PayPal or Apple Pay are steadily on the rise. However, these companies use the collected data not only to facilitate transactions but also to generate customer profiles which allow specific targeting by advertisers.

In the context of Big Data electronic payment information can be used to accurately predict fraud or unauthorised transactions which are outside the normal usage pattern of an individual. By relying on the power of such accumulated information the service and

its security can be immensely improved. On the downside, however, the collected data also creates risks if it is disclosed or used by an unauthorised person. Thus, appropriate access safeguards are necessary similar to the ones used in banks. Many new startups entering the electronic payment market are not aware of the amount of security required as their focus is initially only on rolling out a new payment service.

3 Legal framework of government access rights

Governments around the world have always tried to intercept all forms of communication. This assessment is as applicable to electronic communications as it was to postal mail a century ago. Devices today collect a wide range of data about our surroundings including GPS, humidity, alteration, sounds, power and device usage patterns and movements. With this information alone governments are able to discern patterns through Big Data processing and highlight irregularities which can then be explored in more detail.

National laws and in particular constitutional protections set the boundaries as to the level of surveillance that is allowed within a country. This area of surveillance is the most controversial topic as essentially the citizens of a country are subjected to a general surveillance of their private lifes without their being any form of reasonable suspicion that any of them has committed or will commit a criminal offence. Such measures are subject to narrow restrictions and require a warrant by a judge in the EU to implement certain surveillance measures but do not go so far as to allow the preventative collection of all data for an unspecified purpose. The Data Retention Directive which allowed for a limited storage of communication metadata was found to be in violation of EU law by the European Court of Justice based on its undefined boundaries.[9]

3.1 United States (US)

3.1.1 General legal framework

The US present a unique situation based on their strong constitutional protection of civil liberties. However, these rights are not absolute and subject to various limitations that have been derived from their interpretation by the US Supreme Court. In particular the protection against unreasonable search and seizure of information has become a new area of research and interpretation over the last 50 years. A key distinction which must be observed in this regard is that the protection afforded by the constitution against search and seizure of information is only applicable to actions by the government and does not protect against actions by private enterprises. For this last group one must look to the US Privacy Act as well as applicable state laws.

In contrast to the EU the retention of metadata and the filtering of communication content have been carried out with approval of FISA Courts in the US since 9/11. The Patriot Act[10] and Foreign Intelligence Surveillance Act (FISA) allowed for such measures which forced companies such as Google, Facebook and telecommunication providers to grant the US government agencies (mainly the NSA) access to their facilities or to provide them with data upon request. Many legal scholars have argued that such access rights violate the US Constitution which protects citizens from unreasonable searches.

In Whalen v. Roe[11], the Court highlighted that there are mainly two types of privacy interests that are constitutionally protected: "One is the individual interest in avoiding disclosure of personal matters, and another is the interest in independence in making certain kinds of important decisions." The right to informational privacy, however, "is not absolute; rather, it is a conditional right which may be infringed upon a showing of proper governmental interest".[12]

Constitutional privacy protection only extends to "the most intimate aspects of human affairs" and that a person's "legitimate expectation of privacy" bears on the constitutional analysis.[13] In this context for example "mandatory disclosure of an individual's Social Security Number (SSN) to the Department of Motor Vehicles does not threaten the sanctity of individual privacy so as to require constitutional protection", and constitutional privacy rights only apply to more personal matters such as marriage, procreation, family.[14] Despite the varying judgments the issue of privacy remains a contested one. Each individual case has different facets potentially resulting in decisions based on the weighing of the privacy impact.

3.1.2 Surveillance

Section 215 of the Patriot Act contained the business records rule which allowed the FBI to request any tangible thing if it is relevant for an international terrorism investigation. However, the data could not relate entirely to a US citizen and needed to be approved by a secret court proceeding. In reality the Congressional Oversight Committee over the surveillance program has not stepped in although the amount of surveillance has exponentially increased over the last decade. Scholars have also criticized that such a small Committee is inappropriate in view of the expansive infringement of fundamental rights carried out by the government.[15]

Nevertheless, in view of the documents Edward Snowden released US Congress needed to act. Thus, the Freedom Act was passed on June 2, 2015 which reauthorised the previous powers under the Patriot Act that had expired on June 1 with a few changes and additions. These changes included a stop to the bulk collection of metadata under the Patriot Act and the old case of Smith v. Maryland, 442 U.S. 735 (1979). Furthermore, the large-scale, indiscriminate collection, such as all records from an entire state, city, or zip code is now also prohibited. However, National Security Letters can still be issued by the FBI for a specific person and are subject to non-disclosure requirements. In contrast to the previous rules the non-disclosure requirements must be evaluated in regular intervals and lifted if no longer required. Challenging the non-disclosure is now also possible under the right to judicial review of which the recipient must be informed.[16] Importantly even if a party is subject to a non-disclosure rule it can now still publish information on the amount of requests received and granted in brackets of 1000.[17] This right to publish such data has been taken up by all major IT companies by displaying such information on their websites.

The recent issue of Apple's IPhone encryption and the rejection by Apple to supply the capabilities to decrypt such a phone to the FBI has raised two important issues, namely firstly whether a company can be forced to supply such information and assistance and secondly whether the information gained may be used as evidence in a later trial. Considering the first question, companies are generally required to aid any criminal investigation. However, the judge is left with a wide discretion whether to grant certain orders. The prosecutors in most cases rely on the 1789 All Writs Act which allows

a federal judge to "issue all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of law". The requirements of being 'necessary and proportionate' were included in order to safeguard against limitless powers which could lead to tyranny. In the case of United States v. New York Telephone Co.[18] a three prong test was introduced laying out the requirements for the cooperation of parties. Thus a company subject to an order must

1 be related and not 'removed' from the case

2 the order must not place an unreasonable burden on the company

3 the company's assistance must be necessary.[19]

In light of the technological changes that have occurred since this case the need for reinterpretation taking into account today's vast data collection and sharing seems warranted.

However, as the disclosure of information under the court order is not subject to any secret proceeding such as the National Security Letters[20] the information gained through the assistance of the company in question is admissible in a criminal trial. The admissibility can be challenged as in any criminal proceeding. As long as the New York Telephone Company precedent remains a challenge of the order will not be successful unless one of its elements has not been satisfied.

3.1.3 Emergency procedures

Additionally, the Attorney General was once granted an emergency authorisation to order the release of information when there is no time to apply to the court.[21] If the order is later not approved by a judge the information gathered cannot be used as evidence in court nor in any other setting. In order to enshrine a more citizen-based exercise of surveillance powers the courts must appoint five persons based on their expertise which can act as amicus curiae during court proceedings and advise the judges on civil liberties, communication technology, intelligence collection or other area relevant to the issue before the court.[22]

3.1.4 Airplane travel

Generally, after passing of the Freedom Act the surveillance of US persons is subject to tighter regulation and oversight than previously under the Patriot Act. The limitations imposed on the measures of government agencies also extend to non-US persons after they have been within the USA for more than 72 hours.[23] Creating such as protection is in line with the boundaries set by the US Constitution. This compromise was reached in order to be able to monitor suspected terrorists after they enter the country giving the FBI enough time to apply for a warrant allowing surveillance.

As of June 2015 the FISA courts must publicise how they interpret the law such as the definition of 'specific selection term', which is a core definition preventing bulk data collection. This term requires a clear identification of an individual in order to allow surveillance measures.

3.2 Australia

Australia has passed the Telecommunications (Interception and Access) Amendment (Data Retention) Act which mandates data retention of two years for communication metadata. This includes location, IP and login information. Previously, metadata was only collected for billing purposes by telecommunication providers which deleted the data according to their own internal rules. The law has been heavily criticised as being exceedingly vague and thus leaving an enormous potential for expansion. Importantly the disclosure of the data does not require a warrant which already has been the case previously under Sec. 178 of the Telecommunications (Interception and Access) Act 1979.

Without clear boundaries and oversight such a metadata program is bound to infringe personal privacy in a serious fashion and carries a great risk of abuse. Interestingly, Malcolm Turnbull, the former Australian Communications Minister and later Prime Minister, has given advice to circumvent the Act by using services that do not create metadata such as WhatsApp, Facetime or Skype. By using these services the ISP can only determine the connection to the foreign server, not with whom the communication took place. Additionally, the information gained through the PRISM program in the US and the lack of any clear evidence that the metadata collection program ever prevented any major criminal activity have raised questions in respect of its real need.[24] Thus, already this law is said to be a 300 million Australian Dollar 'White Elephant' a term used for a law without value.

3.3 EU

In the EU as well as in Switzerland the common method to obtain information about an individual is through a court order which allows interception of communication and identification of an individual's communication. For example the UK Regulatory Investigatory Powers Act (RIPA) 2000 regulates targeted surveillance by requiring a warrant to be issued by the Home Secretary before private communication can be intercepted.[25]

Based on the controversial surveillance discussions Europe has recently placed strong limits on the powers of government agencies to use data. In April 2014 the European Court held that the Directive regulating the storage of user identification data is contrary to EU privacy laws as its objective and scope are too broad. The EU member states are obliged to determine how they will implement a framework which is least privacy invasive whilst still ensuring that the investigating authorities have the required data to combat criminal activity.[26] In addition, a new information sharing Directive between police authorities is currently being debated on the European level enabling the sharing of government data on criminal activities.[27]

Commonly information on an individual can be obtained through a court order which allows collection of data and identification of an individual's communication patterns. For example the UK Regulatory Investigatory Powers Act (RIPA) 2000 allows targeted surveillance under a warrant to be issued by the Home Secretary.

In international air travel from Europe a Passenger Name Record (PNR) system is used to identify passengers. These databases contain all personal (i.e. credit card details, address) data which is entered upon booking. The purpose for collection at this point is purely to offer the service.[28] Since 9/11 the US has increased its passenger monitoring for

which it entered agreements with the EU to access the passenger data of the flights coming from Europe. In order for the EU authorities to also benefit from this data the EU Commission has proposed a new EU PNR framework. The implementing law would allow the tracking of all passengers in real-time as well as retrospective flight and other pattern analysis by EU authorities.

As the data is collected for commercial purposes only the tracking of passengers stands in contrast to the purpose limitation principles enshrined in EU data protection laws.[29]

A further concern for privacy advocates is the proposed retention period of up to five years for such data which does not seem warranted in light of the much lower retention periods for internet data currently in force in the EU Member States. As safety measure the anonymisation of the data is required after 30 days which, however, does not prevent the re-personalisation at a later point as it is carried out in a manner which is reversible. By only partially anonymising the data its value is retained.[30] A further growing concern is the ability of the executive to access this data by way of subpoenas or other legal instruments. As the data is purely commercial the handing over of such data should only be required subsequent to a case by case assessment.

4 Privacy protection in the US, Australia and Europe

As starting point of any data privacy analysis the applicable national law to the data must be determined. Potentially relevant are fundamental rights protections, data protection statutes, specific privacy laws as well as sector or industry regulations. In addition, contract and consumer protection laws set boundaries to the extent a private individual can contract out of his or her rights. A further crucial distinction must be made between the public law (the powers the government has over data) and the private sector companies with their abilities to collect and use personal data for commercial purposes.

Over the years various global guidelines have been published by international organisations such as the UN, but only the 1966 International Covenant on Civil and Political Rights (ICCPR) is legally binding on state legislators.[31] The Human Rights Committee interpreted the ICCPR to ban any public interest justification for the infringement of human rights and fundamental democratic tenants.[32] Furthermore, the European Court of Human Rights has clarified the application of human rights to individual cases arising in relation to European member state laws.[33]

4.1 Privacy protection through data protection law

4.1.1 Overview

Various laws impact the collection and use of data as well as the tracking of devices. In order to determine the level of protection and the measures afforded to the users a detailed understanding of the technical processes underlying the data use is necessary. This is particularly the case when intellectual property rights or data protection concerns are involved.

Data protection laws are the primary laws governing the collection and use of personal data. These laws were passed by various legislators in Europe, Australia and the US in order to protect individuals from the use of their most personal information.

However, the scope and depth of the laws vary heavily based on a different understanding of privacy and the need for protection. Often the argument is made that the data can be anonymised thus a collection of DNA data presents an acceptable low risk. Only the actual personalisation of the data should be subject to close regulation and oversight. What such an argument fails to address is the fact that once such vast amounts of data are collected invariably the risk of unauthorised access grows as the security measures required must also keep up with the amount of data stored. Furthermore, if a party steals such information it will not be governed by any form of regulation. Thus only collecting the DNA when this is warranted in the individual case appears to be the most risk averse and prudent solution.[34]

The US has long been an advocate for free speech which forms an integral part of the US Constitution.[35] Logically, the data protection is subject to the right to free speech as well as to the power division between states and the federal government. Today, the US does not have a uniform law for the protection of personal data but has implemented sector specific legislation such as for the use of medical as well as financial information.

In contrast, the EU has gone further in its protection of privacy by having made privacy a fundamental human right according to the EU Charta on Human Rights. Additionally, the General Data Protection Regulation sets strong boundaries for private enterprises and their use of personal data. In particular, the issues of trans-border flow of personal data have been addressed in this Regulation by laying down conditions for such transfers. These aim at ensuring that the data is only processed in accordance with the minimum standards set by the EU data protection law.

Australia has also taken significant measures in the enforcement of data protection, although differently to the EU. In contrast to the territorial view of the EU law the Australian legislator focuses on 13 main privacy principles which must be observed by any company processing personal data wherever this takes place in the world.

4.1.2 The US framework

The USA has chosen to leave the regulation of personal data mostly to the states and only regulate certain sectors such as finance and healthcare as they fulfil the constitutional requirements of touching on interstate trade or commerce or matters which are within the powers of Congress.

Thus, in order to ascertain whether any protection applies to the collected data it must either be shown that a state privacy law applies or that the data falls into one of the categories regulated by the federal government.

4.1.3 The EU framework

In contrast to the US the EU has implemented a new uniform law, the General Data Protection Regulation which harmonises the protection of personal data throughout all member states. It requires certain protections by commercial entities when processing personal data and grants a number of rights to affected individuals such as the right to have their data deleted or updated as well as use limitations placed on it.

4.1.4 The Australian framework

The Australian privacy framework differs from the US and EU as the Privacy Act[36] only applies to private enterprises with over 3 million turnover as well as the federal public sector. In the US and EU the private and public sector are regulated by separate legislation. In addition to the federal Privacy Act, sectoral legislation governs such areas as the communications sector. Furthermore, there are state laws which regulate certain data collection and use. They are intended to be technology neutral and regulate the results of various activities.

The merger of the former Information Privacy Principles which applied to the public sector with the National Privacy Principles (private sector) was carried out in March 2014 as part of a major legislative reform of the Privacy Act. Today the government as well as private actors are subject to 13 Australian Privacy Principles which set out the basis for personal data processing. The jurisdiction of these rules extends even to processing operations outside Australia when an entity carries on a business in Australia or an act or practice is carried out abroad at the time or before personal data was held or collected in Australia. The entity would then be liable as if the breach of the Privacy Act had occurred in Australia.

These Australian Privacy Principles (APP) consist of:[37]

- open and transparent management of personal information
- anonymity and pseudonymity
- collection of solicited personal information
- dealing with unsolicited personal information
- notification of the collection of personal information
- use or disclosure of personal information
- direct marketing
- cross-border disclosure of personal information
- adoption, use or disclosure of government data
- quality of personal information
- security of personal information
- access to personal information
- correction of personal information.

Unless sensitive data is involved the Australian law does not require consent in contrast to data processing laws in the EU unless an exception applies. Only when sensitive information is involved pertaining to one of the special categories such as race, origin, political views, religious belief, sex, membership in unions, criminal records, genetic information or biometric information consent will generally be required for the collection or use of this data. Even if consent is given by the data subject the information must also be reasonably necessary for the one or more of the organisation's functions. Other exceptions are based on specific situations such as the necessity of the data for a legal defence or claim or the collection of the data is required by law.

Importantly, new and controversial areas such as genetic and biometric data have been included in the sensitive data definition alongside criminal records. This step takes account of the risks to the individual the disclosure or unlawful processing of such information can have.

Despite being able to collect personal data more freely than this is possible in the EU, Australian entities are still required to notify the individual of any data collection and use. Such a notice must include essential facts including information on the entity collecting the data and its contact details, the purpose of the collection, the right to gain access and the correction of false data, the identification to whom the data is usually disclosed and whether the data will be transferred abroad and if this is the case to what location.

Contrary to the EU framework, the Australian organisations holding personal data can charge a fee to the individual filing a request for accessing the data. There is no right to request deletion of one's personal data as no requirement of consent exists similar to the EU General Data Protection Regulation that could be withdrawn. However, the organisations must delete data when it is no longer needed for the original notified purpose.

In protecting the personal data the organisation must take all reasonable steps to prevent unauthorised access, processing and alteration of data. What this means in reality varies based on the circumstances of the case and the nature of the personal data.

Third party processing is allowed as long as such action is reasonably expected in the circumstances and the individual must be notified of the collection for such processing. Under the Privacy Act the third party will be subjected to further notification requirements and independent privacy obligations and will be viewed as having collected the data directly from the individual.

APP Rule 8 regulates the transfer of personal data to third countries. Before such a transfer can take place the transferring party must take reasonable steps to ensure that the recipient of the data will not breach the APP as the Australian entity will be held liable for any conduct by the foreign party. Reasonable steps in ensuring compliance include data transfer agreements. However, in contrast to the EU, Australia has not approved of any standard clauses or contracts. Furthermore, no approval of the agreements is required by the Office of the Australian Information Commissioner (OAIC).

Transfers are thus permissible when reasonable steps are taken such as for example having a legally binding agreement in place. Further steps are necessary to ensure that the processing actually complies with the Australian law. These measures include appropriate due diligence and ongoing auditing of the third party's processing operation abroad.

The OAIC has the power in case of a breach to determine that the complainant is entitled to a specific amount of compensation. Furthermore, it may also apply to the federal court for an order that the organisation has breached a civil penalty provision. In such a case the court will conduct a hearing de novo. The maximum penalty for a breach is comparatively low with a maximum fine of 1.7 million AUD for a breach by a corporation whereas the EU General Data Protection Regulation allows for a fine of up to 4% of the worldwide turnover of the concerned enterprise.

Currently, a Bill on Privacy Alerts is pending[38] before the Australian parliament which, if passed, will mandate certain notification requirements in cases in which there has been a data breach. This requirement will ensure that the affected individuals are given the opportunity to limit their potential exposure by changing passwords or blocking credit cards. Although there is a general agreement as to the need for mandatory breach

notification laws the scope as well as the definitions are strongly debated as they may produce a regulatory overload if implemented in a broad fashion. Currently, further notice obligations exist for certain businesses such as in the financial or healthcare sector requiring prompt disclosure of any privacy breach to the supervising authorities.[39]

5 New media challenges and solutions

5.1 International developments

The last few years have seen an exponential rise of social media services enabling the fast and open interaction between people in the online word. These services not only include communication tools such as Snapchat or Facebook but also video and photo services which enable the users to upload digital content. YouTube and Instagram are currently the market leaders in this regard with substantial revenue being derived from targeted advertisements. Generally, the use of such services is open to anybody above 13 years of age. This is the age set by the US Children's Online Privacy Protection Act (COPPA) for collecting information on users. Additionally, most US based service providers have implemented such an age requirement in their Terms of Service. For example YouTube uses such a policy as many of the videos are uploaded by minors. Some of the videos are educational or for fun, others are very personal and reveal a lot of information about the individual.

Underage postings on such sites present a particular challenge for the service providers as they have to deal with various laws in force at the location from which the data is uploaded. The contract will in most cases specify the seat of the dispute to be California and the applicable law to be Californian law, however, if there is a dispute as to capacity of the minor as well as criminal law questions these will invariably be subject to the law at the place of residence of the minor. YouTube has implemented automatic systems that take down videos that infringe copyright (music, video content) or do not comply with the terms of use (nudity etc.). However, these tools only catch a certain amount of data and do not entail special protection for minors.

This young user group between 13-18 years is highly at risk as its members are not fully aware of the privacy risks certain postings can create or are not mature enough to determine what content can be uploaded safely and will not lead to unwanted effects in the future. Furthermore, it seems unlikely that such users will be able to understand the standard contracts which they accept when signing up to the website. Essentially minors cannot enter into legally binding contracts which are not covering necessities or approved by their parents. As there is no mechanism to ensure the real age of the party signing up to a service this group of users is left at risk. A higher level of scrutiny seems warranted for these underage user accounts. The main question remains how the gap between the protection of young users and the varying legal frameworks applicable to this content can be bridged.

The first measure that should be taken by the government is to improve education on the use and risks of online media. Before limiting the use of a service or placing restrictions on it teenagers must be made aware of the inherent risks various media outlets create. This requires resources in schools as well as parental engagement at home in order to educate on how to properly use various online services, many of which are highly beneficial for social interaction fostering charity, volunteering, artistic endeavours as well

as exposure to a diverse range of people. On the downside, risks are created through inappropriate content, lack of understanding of online privacy issues, third party advertising as well as through peer to peer interaction. Cyber bullying is one of the examples of such peer to peer harassment that is carried out online.[40] In recent times the sending of sexually explicit messages has also drawn attention in the media. Additionally, the regular use of media services creates challenges for individual privacy because often too much personal information is shared and made available on such sites. Media consumption also creates its own health risks such as Facebook depression or addictive behaviour which can lead to symptoms such as sleep deprivation.

Targeted advertisements are very controversial when they cater to teenagers. Often they pressure the person into buying a product which he or she does not need and feels obligated to buy because of peer pressure. The teenager must learn to understand that any promotion of a good or service is tailored to his current situation making him more susceptible. With this knowledge in mind it is easier to resists and to make informed choices.

5.2 Data removal and the right to be forgotten

The right to be forgotten is not an absolute right according to the CJEU as it depends on "the nature of the information in question and its sensitivity for the data subject's private life and on the interest of the public in receiving that information, an interest which may vary, in particular, according to the role played by the data subject as part of public life".[41]

5.2.1 US

California for example has implemented a law in 2015 that requires operators of a website or an online service to delete data that has been uploaded by a minor on request of that minor.[42] However, this requirement is only applicable until the minor reaches the age of 18 at which point the request can no longer be enforced. This limitation seems to contradict the reality which is that only long after the material was posted the adult will later regret these actions at which point no mandatory deletion will be enforceable. Although the action of uploading the data was carried out as a minor he/she will not be able to have the data deleted once he/she is a prudent adult who is fully able to understand the effects the posted information has on his or her live.

5.2.2 Australia

The Australian Law Reform Commission (ALRC) has published a report on the issue of keeping the records of underage children confidential. It concluded that the individual situation must be closely analysed in order to determine whether there is a reasonable expectation of privacy. Special information such as counselling and health reports carry an expectation of privacy whereas academic performance reports are expected to be shared with the parents of a pupil. Thus, it is essential for schools and other parties that store personal information of minors to ensure that their policies on information sharing are clearly communicated and disclosure is only made when it is reasonable, necessary, and does not contradict the reasonable expectation of the minor.

5.2.3 EU

In contrast to the US, the EU allows for the right of the data subject to have his or her data deleted based on a withdrawal of consent to the processing or an objection to the processing based on the grounds of public or legitimate interest.[43] Thus, the user of a social media service can at any time withdraw his consent to the processing under the agreement with the provider. Furthermore, where consent has been given by a minor the question will remain as to the validity of the consent to the processing. However, the extent of the right to object to the processing strongly depends on the nature of the data and the service offered. Often the right to an uploaded video is granted to the media site and thus is subject to the contract between the parties. In these instances the data subject may only be able to have his personal data deleted because the right to the digital media was transferred to the service offeror.

5.3 Privacy by design

Privacy by design is currently promoted as the industry's self-regulating solution to the privacy issues generated by Big Data and other cloud based technologies.[44] At its core it implements basic data and privacy protection mechanisms into the functioning of the technology and ensures privacy is maintained by default. From a hardware perspective this functions in the background without the user noticing anything. However, the software is far more flexible and requires constant updates and adjustments to be compliant with the privacy requirements set by the customer.

In the context of social media and video sharing sites, Privacy by design would allow the user to be certain that the basic settings are private and that only the content which is actively set to public is made available to other users. Despite such measures the aim and goal of these websites and services is to promote sharing and without using these functions there is no need to sign up. Thus, it is more a question to what degree a person wants to share personal information on these sites.

Determining what data is shared and how to protect oneself when using various media services should be made as easy as possible considering the wide range of users (inexperienced to tech savvy).

5.4 Tor Systems

In order to reduce the risks of international terrorism and cyber-attacks the US government monitors all traffic to and from federal agency websites. A sign warns users that their use of the site is monitored and, consequently, there is no reasonable expectation of privacy which would protect such communication.[45] Re-routing and anonymisation tools can prevent most standard surveillance technologies. Tor presents a simple solution which anonymises the routing of the data sent and received. Its aim is to prevent a party from identifying the receiver or sender of the transferred data.[46] However, the US government has already tried to gain access to the Tor system and has expressed its view that the system is illegal as it allows criminal activities. Additionally, the system slows down processing which most private users are not willing to accept in return for more security. New data suggests that malware sites allow the government to install programs which enable the identification of users even when they are using a Tor system.

Such measures were previously only used in specific instances but seem to have become common practice in the FBI's daily dealings.[47]

Spyware and other programs are the new tools of choice for surveillance agencies around the world.[48] They allow unnoticed access to most personal computers and even sophisticated server systems. The information that can be gained by such measures is highly valuable as it allows the detection of treats without the other party noticing. Because of the malware's potential to damage a computer system and open backdoors for other parties beside the surveillance agencies its use should be strictly limited to specific targets (as is currently the case in Switzerland) and not applied uniformly on any system that can be infected.[49]

6 Outlook

The risks inherent in media usage has increased significantly not only for journalist, whistle blowers and other parties that are in the public eye but also for the individuals who use electronic media on a daily basis. Thus, individuals must re-think the way in which they use such media and implement appropriate technical safeguards in order to limit their privacy risks. Furthermore, legislators have to design appropriate legal frameworks granting the individual the right to determine which data can be disclosed and to whom.

However, it seems that although steps are being undertaken to limit privacy infringements by private entities through laws such as the European Data Protection Regulation public data access is still an insufficiently regulated area of law. Often states are allowed to intercept communications based on a wide range of exceptions, thus heavily infringing on the right to privacy as well as on the freedom of speech. In this regard judicial approval and oversight is essential in order to limit the use of surveillance to the absolute necessary and to ensure that the information gained is deleted once it is determined not to be relevant. Rising awareness in society is central to a more robust privacy discussion and the design of a framework which addresses privacy concerns as well as efficiency and public security.

Notes

1 See, e.g., http://techterms.com/definition/media (accessed 2 January 2017).

2 Australian Law Reform Commission, The Privacy Act: Some Important Definitions [online] http://www.alrc.gov.au/publications/6.%20The%20Privacy%20Act%3A%20Some%20Important%20Definitions/what-%E2%80%98personal-information%E2%80%99 (accessed 2 January 2017).

3 See, e.g., Alex Castle, Leave no trace: Tips to cover your digital footprint and reclaim your privacy [online] http://www.pcworld.com/article/2143846/leave-no-trace-tips-to-cover-your-digital-footprint-and-reclaim-your-privacy.html (accessed 2 January 2017).

4 Eckersley, P. (2010) 'How unique is your web browser?', *Proceedings of the 10th International Conference on Privacy Enhancing Technologies*, p.1, Springer-Berlin.

5 Eckersley (note 4), p.2.

6 https://www.ghostery.com/ (accessed 2 January 2017).

7 For example Hotspot Shield has such a provision which do not class IP addresses as personal data [online] https://www.hotspotshield.com/privacy/ (accessed 2 January 2017).

8 Yokubaitis, S. (2016) 'You are the product: the price of free in the growing privacy industry', *GoldenFrog*, 12 January [online] goldenfrog.com (accessed 2 January 2017).

9 Joined cases C-293/12, Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and C-594/12, Kärntner Landesregierung, Judgment of 8 April 2014.

10 Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act) Act of 2001; [online] http://www.gpo.gov/fdsys/pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf (accessed 2 January 2017).

11 429 U.S. at 598–99, 97 S.Ct. 869, 51 L.Ed.2d 64 (1977).

12 Doe v. Attorney General of U.S., 941 F.2d at 796 (1991).

13 Eagle v. Morgan 88 F.3d at 625 C.A.8 (Ark.),1996.

14 Stoianoff v. Commissioner of Motor Vehicles, 107 F.Supp.2d 439 (S.D.N.Y.2000).

15 Dana Post, Congressional Oversight of Intelligence Criticized. Washington Post 27.04.2004, [online] https://www.washingtonpost.com/archive/politics/2004/04/27/congressional-oversight-of-intelligence-criticized/a306890e-4684-4ed4-99a0-c8ae7f47feb7/ (accessed 2 January 2017).

16 Sec. 502 (g) Freedom Act.

17 Sec. 603 Freedom Act.

18 United States v. New York Telephone Co. 434 U.S. 159 (1977).

19 Ibid, 175.

20 For a detailed discussion see: Rolf H. Weber/Dominic N. Staiger. Spannungsfelder von Datenschutz und Datenüberwachung in der Schweiz und in den USA, in: Jusletter IT 15. Mai 2014.

21 Sec. 102 Freedom Act.

22 Sec. 401 Freedom Act.

23 Sec. 701 Freedom Act.

24 Bailey Cahall/David Sterman/Emily Schneider/Peter Bergen, Do NSA's Bulk Surveillance Programs Stop Terrorists?, International Security Policy Paper 2014, https://www.newamerica.org/international-security/do-nsas-bulk-surveillance-programs-stop-terrorists/ (accessed 2 January 2017).

25 Regulatory Investigatory Powers Act 2000, Articles 6-11.

26 Judgment in the joint cases C-293/12 and C-594/12, Press statement Nr. 54/14 Luxemburg, den 8. April 2014 http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054de.pdf (accessed 2 January 2017)

27 Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties and the free movement of such data [online] http://db.eurocrim.org/db/en/doc/2366.pdf (accessed 2 January 2017).

28 European Commission, Communication from the Commission on the Gloabal Approach to Transfers of Passenger Name Record Data to Third Countries, European Commission, Brussels 2010, 3.

29 Article 29 Working Party, European data protection authorities clarify principle of purpose limitation, Brussels, 08 April 2013, [online] http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/20130408_pr_purpose_limitation_en.pdf (accessed 2 January 2017).

30 See second report on the proposal directive of the European Parliament and of the Council on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crimes, Article 9.2 [online] http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A8-2015-0248+0+DOC+PDF+V0//EN (accessed 2 January 2017).

31 Weber, R.H. and Heinrich, U.I. (2012) *Anonymization*, p.25, Springer Briefs in Cybersecurity, Cham.

32 Human Rights Committee, International Covenant on Civil and Political Rights, 102nd Session, 12 September 2011, CCPR-C-GC/34, No. 23.

33 See Article 8 ECHR.

34 Rauhofer, J. (2014) 'Round and round the garden? Big data, small government and the balance of power in the information age, in Schweighofer/Krummer/Hötzendorfer (Hrsg.), *Transparenz*, IRIS 2014, Vienna 2014, 607, 611.

35 Vgl. Tinker v. Des Moines Independent Community School District, 393 U.S. 503 (1969).

36 Privacy Act 1988 [online] https://www.legislation.gov.au/Series/C2004A03712 (accessed 2 January 2017).

37 Office of the Australian Information Commissioner, Privacy fact sheet 17: Australian Privacy Principles [online] https://www.oaic.gov.au/individuals/privacy-fact-sheets/general/privacy-fact-sheet-17-australian-privacy-principles (accessed 2 January 2017).

38 Privacy Amendment (Privacy Alerts) Bill 2014 (Cth).

39 See for example Health Insurance Portability and Accountability Act of 1996 [online] https://www.gpo.gov/fdsys/pkg/PLAW-104publ191/html/PLAW-104publ191.htm (accessed 2 January 2017).

40 For detailed figures and research on cyber bullying see [online] http://cyberbullying.org/what-is-cyberbullying/ (accessed 2 January 2017).

41 Weber, R.H. (2015) 'On the search for an adequate scope of the right to be forgotten', *JIPITEC*, Vol. 6, No. 2, pp.2–10; Lee, D. (2014) 'What is the 'right to be forgotten'?', *BBC News*, 13th May [online] http://www.bbc.com/news/technology-27394751 (accessed 2 January 2017).

42 Privacy Rights for California Minors in the Digital World S.B. 568 [online] https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201320140SB568 (accessed 2 January 2017).

43 EU Data Protection Regulation, Article 6,17,19.

44 Schaale, C. *How Cloud Providers are Adopting Privacy by Design* [online] http://policyreview.info/articles/news/how-cloud-providers-are-adopting-privacy-design/336 (accessed 2 January 2017).

45 US Department of Homeland Security, National Cyber Division, US Computer Emergency Readiness Team, Privacy Impact Assessment: Einstein Program. Collecting, Analyzing and Sharing Computer Security Information across the Federal Civilian Government, September 2004.

46 [online] http://www.torproject.org/torusers.html.en (accessed 2 January 2017).

47 Poulson, K. (2014) 'Visit the wrong website, and the FBI could end up in your computer', *Wired*, 8 August [online] http://www.wired.com/2014/08/operation_torpedo/ (accessed 2 January 2017).

48 Federal Business Opportunities, Solicitation Number: RFQ1307A [online] https://www.fbo.gov/index?s=opportunity&mode=form&id=5b4b8745e39bae3510f0ed820a08c8e2&tab=core&_cview=0 (accessed 2 January 2017).

49 Weber, R.H. and Staiger, D.N. (2014) *Spannungsfelder von Datenschutz und Datenüberwachung in der Schweiz und in den USA*, 15 May, in Jusletter, IT.