Available online at www.sciencedirect.com

ScienceDirect

www.compseconline.com/publications/prodclaw.htm

Computer Law & Security Review

The digital future – A challenge for privacy?

Rolf H. Weber *

University of Zurich, Switzerland

Keywords:
Privacy concepts
Privacy issues
Regulatory measures
Technological solutions

ABSTRACT

Increasingly, data protection laws and the concept of privacy are subjected to manifold challenges created through advancing new technologies such as Big Data, digital identity, biometrics and social media sites. Such technological shifts, although being immensely beneficial to society at large, create problems for the protection of an individual's privacy. This article addresses the arising issues and suggests innovative technological solutions for minimizing privacy infringements and negative impacts on the private sphere of individuals.

1. Introduction to privacy concepts

Privacy protection in Europe follows a long tradition. As part of the European Convention on Human Rights,[1] national constitutions of EU Member States[2] and the Charter of Fundamental Rights of the European Union[3] (CFREU) the right to privacy forms a foundation for the European Member States' data protection legislations. Increasingly, however, these laws and the concept of privacy are subjected to manifold challenges created through advancing new technologies such as Big Data,[4] digital identity, biometrics and social media. These technological shifts, although being immensely beneficial to society at large, create problems for the protection of individual privacy. This article addresses the present issues and suggests innovative technological solutions for minimizing privacy infringements and negative impacts on the private sphere of individuals.

The first part of this paper highlights the current privacy issues created by various forms of new technologies. In the second part technological solutions are proposed to counteract the identified privacy risks and the boundaries of such measures are analyzed. In particular the ability of an individual to consent to privacy infringements as a way of allowing the service provisioning poses a question of accountability and power abuse. Currently, users are "paying" for services by making available their personal data. Therefore, as a potential solution clear rules must be established on the steps required to inform a user of the data's utilization by the provider as well as third parties.

* Chair Professor for International Business Law at the University of Zurich, Visiting Professor at Hong Kong University, Attorney-at-Law in Zurich, Switzerland.
E-mail address: rolf.weber@rwi.uzh.ch.

[1] European Convention on Human Rights and Fundamental Freedoms, 01.06.2010, <http://www.echr.coe.int/Documents/Convention_ENG.pdf>.

[2] Charter of the Fundamental Rights of the European Union, (2000/C 364/01), 18.12.2000, <http://www.europarl.europa.eu/charter/pdf/text_en.pdf>.

[3] Charter of Fundamental Rights of the European Union (2000/C 364/01), 18.12.2000, <http://www.europarl.europa.eu/charter/pdf/text_en.pdf>.

[4] Big Data usually includes data sets with sizes beyond the ability of commonly used software tools to capture, curate, manage, and process the data within a tolerable elapsed time. See Chris Snijders/Uwe Matzat/Ulf-Dietrich Reips, (2012) 'Big Data': Big gaps of knowledge in the field of Internet. International Journal of Internet Science, 7, 1–5. <http://www.ijis.net/ijis7_1/ijis7_1_editorial.html>.

http://dx.doi.org/10.1016/j.clsr.2015.01.003

2. Current privacy protection frameworks

2.1. *Fundamental rights*

Fundamental rights are key to the international legal framework and touch upon an individual's right to privacy. However, in practice these rights are not yet sufficient to cater for the privacy challenges faced in today's online world. Additional national laws are necessary to extend the essential privacy protection to new technologies and scenarios currently emerging.

In Article 1 of the UN Universal Declaration of Human Rights[5] (UDHR) as well as in the CFREU the protection of human dignity is a central concept. Furthermore the European Convention on Human Rights contains an express protection for privacy of individuals applying not only to government but also to private actors. Thus, appropriate privacy laws must be implemented in all countries to ensure the protection of these fundamental rights.

Privacy infringements can occur in various forms either by an individual directly disclosing information to a third party on a social networking website or by a commercial entity collecting the data for business purposes. This paper is concerned with the second of these scenarios as private disclosure is more likely to be acceptable within certain boundaries.

2.2. *Specific laws*

The US approach to privacy is primarily derived from constitutional protections which have been expanded over the last decades to include certain aspects of private conduct. Furthermore, in addition to state data protection legislation federal laws are in place in certain areas such as for the protection of medical data.[6] Recently the topics of surveillance and privacy have gained traction based on the Snowden revelations.

Already in 2011 a push for better privacy protection had been undertaken by introducing the Do Not Track Me Online Act of 2011[7] which aimed at enhancing customer rights in order to limit the use of their personal information by commercial entities. Due to a lack of a majority in Congress the introduced law has not been passed yet. However, fresh legislation action is being taken by Congresswoman Speier to introduce a new Mobile App Privacy Protection Act[8] which aims at the privacy issues created by the tracking functions in mobile phone applications. The Act would ensure that users of mobile services are made aware of the type and extent of the data being collected from them as well as their options in limiting disclosure by adjusting their mobile phone settings. Importantly the Act would also allow for civil actions and potentially even class actions against the app-providers which do not follow the disclosure provisions.

Currently, there are various class actions before US courts based on the controversial topic of preventing companies from tracking their users.[9] California has passed such a "Do not Track Law" requiring the companies to inform their customers whether they conform to rules supplied by browsers signaling that the user does not want to be tracked or referring the consumer to choice options of the provider. This also includes the requirement to disclose third party tracking on a website.[10] The US Federal Trade Commission (FTC) has issued guidelines on the subject.[11]

The FTC has long realized that most commercial providers of online services, falling outside the scope of specific privacy legislations, such as for the protection of children under the age of 13, do not adequately inform their customers of their collection practices.[12] In its 2012 report the FTC has therefore recommended to Congress "*that* Congress enact legislation to implement a Consumer Privacy Bill of Rights based on the Fair Information Practice Principles[13] ("FIPPs")".[14]

In Europe these issues have not yet been specifically addressed by way of sector-related legislations. However, the Article 29 Working Party (an advisory group to the European legislator) has raised the privacy issues created by apps in a working paper.[15] In particular it highlighted that only 61% of the top 150 apps provide a privacy policy to the customer.[16] Furthermore, no real choice is given to the app-user for raising objections against the terms and conditions once the software is downloaded. In most cases, only a simple box is left for the

[5] UN Universal Declaration of Human Rights <http://www.un.org/en/documents/udhr/>.

[6] U.S. Department of Health & Human Services, Privacy Protection, <http://www.hhs.gov/ocr/privacy/index.html>.

[7] Bill Text 112th Congress (2011–2012) H.R.654.IH <http://thomas.loc.gov/cgi-bin/query/z?c112:H.R.654.IH:>.

[8] Congresswoman Speier commits to introduce such a legislation in the 113th Congress <http://speier.house.gov/index.php?option=com_content&view=article&id=203:protecting-your-consumer-rights&catid=10:issues&Itemid=46>.

[9] For example the $14 million settlement in Harris v. comScore, No. 11 C 5807, <http://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?article=1338&context=historical>.

[10] Dominique Shelton, Inside Calif.'s Proposed Guidance for Do-Not-Track Law, <http://www.law360.com/articles/496938/inside-calif-s-proposed-guidance-for-do-not-track-law>.

[11] FTC, The Do Not Track Option: Giving Consumers A Choice, <http://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/do-not-track>.

[12] FTC, Privacy Online: Fair Information Practices In The Electronic Marketplace, May 2000, <http://www.ftc.gov/sites/default/files/documents/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission-report/privacy2000.pdf>.

[13] White House, Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy (Feb. 2012), <http://www.whitehouse.gov/sites/default/files/privacy-final.pdf>. The FIPPs as articulated in the Administration paper are: Transparency, Individual Control, Respect for Context, Security, Access, Accuracy, Focused Collection, and Accountability.

[14] Protecting Consumer Privacy in an Era of Rapid Change, FTC Report 2012, 3, <http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf>.

[15] Article 29 Working Party, Opinion 02/2013 on apps on smart devices, 6, <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp202_en.pdf>.

[16] FPF Mobile Apps Study, June 2012, <http://www.futureofprivacy.org/wp-content/uploads/Mobile-Apps-Study-June-2012.pdf>.

customer to tick and accept the terms. The data collected by apps often far exceeds what is necessary to provide the service.[17]

Furthermore, the EU has proposed a new Data Protection Regulation (DPR)[18] which will address some of the most pressing data protection issues created by new technologies such as smart phones and cloud computing. Particularly it aims at ensuring that the personal data of individuals are protected no matter where or what form of processing is undertaken. From a general legal perspective, indirect regulations also need to be taken into account, such as telecommunications secrecy provisions or confidentiality norms in civil law relationships.

3. Current privacy issues

New technological advances have created an ease in privacy infringement previously unknown. For example Big Data allows for the processing of vast amounts of personal information, behavioral pattern extraction and identification of individuals. Nearly all online services require some form of identification which can be put to various use.

Before creating online accounts for identification purposes a user should consider the risks of placing personal information into the hands of a commercial entity. Many companies are subject to hacker attacks which, if successful, give third parties access to personal and financial information of individuals. A prominent example is Sony which was fined by the UK Information Commissioner for a data breach in 2011 resulting in the access of millions of customer datasets by a group of hackers.[19] Furthermore, these companies could sell the data to interested third parties. For good reasons, therefore, due to an increase of media attention, awareness is slowly growing around the world as to these online risks and the need to implement appropriate countermeasures.

3.1. *Social login*

A social media login is a new social media technology with strong privacy implications and growing importance in daily online dealings. It allows users to create new accounts with service providers by using an already existing social media profile.[20] These profiles often contain a wide range of personal data which are shared to a great extent with the new service upon registration. Although a user can limit the access by the new service to its social media profile the provider almost always sets a minimum requirement of access in order to complete a registration. Thus, the user is faced with either choosing this convenient way of creating a new account via the same login as for the social media site and accepting the disclosure of his information or to create a new account the old fashioned way by entering his personal data. Often the rights granted under such a login include a right to post on behalf of the user information to his social media profile for advertisement purposes.

Some new certificates have emerged which inform the user of the amount of data that will be accessible through the social media login service. As these certificates are not yet established in the market and unknown to the general customer they only provide a protection for those prudent users who are informed of the privacy threats of this system. Thus, it would be advisable to create an international uniform and easily understandable standard of disclosure by such social media login providers which can be grasped by the common user with only general IT knowledge. Furthermore, it is necessary to give the customer a choice in limiting access without totally blocking him from using the benefits of the login.

New services which apply a "uniform login" for most social media and other sites aim at streamlining the login process and making identification more secure. However, even for such a system a password as initial login is required.[21] Thus, once a third party gains access to this code it can freely use a manifold number of services which previously might have had different login information but through the use of social media now are verified through a single password.

3.2. *Third party access to online data*

In addition to the threats of unwanted disclosure through criminal activity privacy concerns arise as to one's personal online identity. Humans portray themselves to various social groups in a different manner. For example in the work related sphere one wants to be seen as intelligent, well mannered, reliable and professional. However, in a more social context such as with long term friends one might want to share more personal stories, pictures and information.[22]

Increasingly, the clear line between these forms of information is blurring as there is an overlap of the content provided online. For example Facebook encourages the sharing of information which requires the display of a person's face as a minimum requirement. Additionally, links are created to profiles in a manner the user cannot always control and which can be found by search engines, ultimately leading to a public profile which was never intended to be created by the individual.

3.3. *Employee online screening*

The data which is put onto social networking sites over the years can generally be found by online search engines. Increasingly employers are using online tools for background

[17] Wall Street Journal, Your Apps Are Watching You, <http://online.wsj.com/article/SB10001424052748704694004576020083703574602.html>.

[18] European Commission, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM(2012) 11/4 draft, 2012, Article 79(6), <http://ec.europa.eu/justice/dataprotection/document/review2012/com_2012_11_en.pdf>.

[19] ICO, Sony fined £250,000 after millions of UK gamers' details compromised, 24.01.2013, <http://ico.org.uk/news/latest_news/2013/ico-news-release-2013>.

[20] Gigya, Simplify User Registration and Login, <http://www.gigya.com/social-login/>.

[21] David Kirkpatrick, Social Media Marketing: Social login or traditional website registration?, 12th January 2012, <http://sherpablog.marketingsherpa.com/social-networking-evangelism-community/social-login-registration/>.

[22] Gerber Macionis, Linda John, Sociology 7th Canadian Ed. Toronto, Ontario: Pearson Canada Inc. (2010) pp. 149, refer to so called primary and secondary social groups.

screening of their prospective employees. Such software takes the information provided in the applicants CV and searches for various online user accounts. It then scans all information including pictures to determine whether the data contains "aggressive or violent acts or assertions, unlawful activity, discriminatory activity (for example, making racist statements), and sexually explicit activity".[23]

Essentially the software tries to ensure the privacy of the prospective employee in regard to legally protected information. In doing so, the software blacks out any information that could relate to a person's ethnicity, sexual orientation, religious affiliation and national origin. It therefore only generates a limited report for the employer where the above mentioned unwanted behavior is found. As the applicant provides the initial data this person is uniquely able to stir the investigation into the desired direction this person wants by providing a new email address which does not exists for a long time and which is not linked to any potentially relevant data.

The automatized process is able to ensure the privacy of the individual as it is free from human bias, focuses only on very specific aspects of the person and is neutral to other factors thus as long as the parameters of the search are set correctly the privacy infringement is minimal. However, when an employer conducts its own research for example by searching for the applicant's name online and finds out information which the employee is not obliged to disclose under normal interview circumstances, the hiring process creates many pitfalls. On the one hand, the potential candidate might become aware of the fact that non-disclosable information such as a pregnancy is known to the employer and thus might give rise to a claim for discrimination, on the other hand, it will be very difficult for the employer not to use this valuable information it acquired through a public search.

Currently in the 113th US Congress a bill for a Social Networking Online Protection Act has been introduced to address the concerns raised in regard to employee information in a social network setting. Particularly the bill expressly prohibits the employer from requiring an applicant or employee to disclose personal login data or the username of a social networking site.[24] These provisions also apply to the academic setting ensuring protection of students from such request by their educational institutions. In addition to the proposed bill some US states have passed their own regulations addressing the issues faced at the intersection of employment and privacy protection law. Germany has not proposed a specific law on the issue; however, the courts have decided that open public accessible information can be used by the employer as this is seen as a public announcement and thus does not receive privacy protection.[25] Nevertheless, any further action needs to be justified and proportionate, thus it will be evaluated on a case by case basis and only applies once the person is actually an employee.

In substance, it is up to the individual to determine whether the personal information provided on a social network site can be accessed by the public at large including the software used by employers to screen potential employees or to decide to block such access through the appropriate settings. If the profile is public an employer will under the proposed new laws still be able to analyze the profile within the boundaries provided for by various employment laws and other limitations. However, it is clear that if the profile is private the employer cannot demand to gain access to such a profile.

If an applicant wants to ensure that his online information is kept to a minimum he should close all social website accounts and then request the major search websites to delete the references to his person.[26] This is a tedious process but currently the only solution since other means are not available. It remains to be seen whether the Google decision[27] in Europe will influence the search engine providers to supply a more efficient means to have one's data deleted. Currently Google is fulfilling deletion requests on a case-by-case basis after an aggrieved party has submitted its request via an online form to Google and has given sufficient reasons for the deletion.[28] Google will then assess whether there are sufficient grounds to delete the information and if public interest would outweigh the deletion right. A newly established advisory committee will support Google in ensuring that the right balance is maintained between the competing interests in such a request.[29]

3.4. *Location data*

Location data of mobile phones are regularly sent to the app-provider and even third parties gain access to this data. Often the terms of service include a provision for the consent of the customer to the disclosure when the service is installed or used. However, recent research has shown that the way in which privacy policies are worded requires an education level of a sophomore to junior in college to comprehend. It is therefore explicable why most users do not understand what they are consenting to as the average reading level in the US is around the level of a 8th to 9th grade pupil.[30] Similar figures are also true for the EU.[31] Thus, such privacy policies do not

[23] Mat Honan, I Flunked My Social Media Background Check. Will You? 07.07.2011, <http://gizmodo.com/5818774/this-is-a-social-media-background-check>.

[24] Social Networking Online Protection Act, <https://www.congress.gov/bill/113th-congress/house-bill/537>.

[25] LAG Hamm, Urteil vom 10. Oktober 2012, Az. 3 Sa 644/12 <http://openjur.de/u/565291.html>.

[26] Andrew Tarantola, How to Erase Yourself From the Internet, 02.11.2013, <http://gizmodo.com/how-to-erase-yourself-from-the-internet-1456270634>.

[27] Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González, ECJ C 131/12 <http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=11654>.

[28] The form is available at <https://support.google.com/legal/contact/lr_eudpa?product=websearch>.

[29] James Vincent, Google begins implementation of 'right to be forgotten' ruling with online takedown form, The Independent 30. May 2014, <http://www.independent.co.uk/life-style/gadgets-and-tech/google-begins-implementation-of-right-to-be-forgotten-ruling-with-online-takedown-form-9459209.html>.

[30] U.S. Department of Education, Adult Literacy in America (NALS). National Center for Education Statistics, U.S. Dept. of Education, Office of Educational Research and Improvement (NCES 1993–275) (2002).

[31] See EU Literacy Report, <http://ec.europa.eu/education/policy/school/doc/literacy-report_en.pdf>.

meet the Federal Trade Commission's general notice provisions as the user cannot make an informed choice.[32]

Practice has also shown that a significant number of apps do not provide privacy policies to their user or send location data without the knowledge of the user.[33] A 2012 study conducted on 2254 adults came to the result that 54% of the app-users would not install an app if they knew about the amount of information that is shared with the app-provider.[34] Additionally 19% of mobile phone users have the location tracking functions turned off because of fear that third parties may be able to access this information. However, even if a Wi-Fi network is used the location can be ascertained by triangulation through the vast number of hot spots available nowadays. This is in line with the developments in GPS stalking which increased to around 10% of the overall stalking complaints in the US in 2009.[35]

Geo-location data (location information from GPS or Wi-Fi Networks) not only has commercial value but can also be used to improve public service and security. It allows for the tracking of a person in need who is dialing an emergency number and does not know their own exact location.

3.5. *Profiling*

Profiling entails the collection of vast amounts of data about an individual. It is used to target advertisements and products more specifically to the needs of the potential buyers. The Article 29 Working Party which consists of members of all the EU Data Protection Authorities has recently made a concerning statement. It said that "where profiling does not significantly affect the interests, rights or freedoms of the data subject, [the rules setting out individuals' right to object to profiling] do not apply and the lawfulness of processing is to be assessed in the light of the other provisions of the [General Data Protection] Regulation."[36]

This Data Protection Regulation (DPR) aims at limiting the use of personal data, especially when legal effects are to be produced for individuals based on an automated processing of their personal data. Such processing will only be possible once consent is given and appropriate safeguards are put into place. However, there are again exceptions to the exceptions: For example consent is not required if the profiling is being carried out for the performance of a contract with the customer or where national laws allow for such processing under appropriate safeguards. Furthermore, the consent is often given without clear intent due to misleading information or problematic technical guidance.

It remains to be seen how the balancing approach the EU Commission is taking in regard to the DPR will present itself at the end. In principle the clear consent of the data subject should be required before any profiling process can be initiated. Any exceptions must be kept to a minimum. Furthermore, the term profiling should be clearly defined in the Regulation.[37] The addition of a data protection impact assessment will also highlight the risks created through a specific data collection and profiling method enabling the companies to further improve their privacy protection mechanisms.

3.6. *Government data*

Increasingly governments are collecting data of their citizens under various administrative laws. These include registrations for cars, residency, taxation as well as financial information, marital status and electricity and water use. The information enables the government agencies to carry out their task more efficiently and increase service levels. However, with the collection of more and more data the risk increases as to its effect on the privacy of an individual when combined with other data or disclosed to the public under a freedom of information request.

Beside ensuring the privacy of individuals through the protection of collected and stored data public agencies should also be regulated in terms of the type and amount of data they are allowed to retain. Furthermore, the use of this data must be limited to specific tasks necessary for the performance of the agency's function. Such a limitation is required as otherwise the use of the data will grow over time diluting the distinction between its use for public services and that of profit orientated enterprises.

There is a general perception within companies and governments that when data is available it should be used. Government agencies are incentivized through a growing need for cost reduction to enable the use of all collected data to make their decision-making process more efficient. Estonia is leading this trend in Europe with an entire e-government system allowing citizens to file tax returns, request social services, vote and carry out many more things entirely online.[38] However, severe security risks arise where this data is collected and controlled centrally. In essence if the system is breached a party could gain access to all relevant information about a person. In addition this data can be used by secret services for targeted action which might violate an individual's privacy rights. Especially minority groups could be targeted through

[32] Caitlin D. Cottril, Piyushimita Vonu Thakuriah, Privacy in context: an evaluation of policy-based approaches to location privacy protection, Int. J. of Techn. Law, Volume 22/2, 190.

[33] Anne S.Y. Cheung, Location privacy: The challenges of mobile service devices, Computer Law & Security Review 30 (2014) 44.

[34] Jan Lauren Boyles, Aaron Smith and Mary Madden, Privacy and Data Management on Mobile Devices, Pew Internet Reports, 5. September 2012, <http://pewinternet.org/Reports/2012/Mobile-Privacy.aspx>.

[35] Katrina Baum, Shannon Catalano, Michael Rand and Kristina Rose, Stalking victimization in the United States, US Department of Justice 2009, 5, <http://www.ovw.usdoj.gov/docs/bjs-stalking-rpt.pdf>.

[36] Out-Law.com, Profiling rules should not apply unless individuals' rights are 'significantly affected', says privacy body, 23. 05.2013, <http://www.out-law.com/articles/2013/may/profiling-rules-should-not-apply-unless-individuals-rights-are-significantly-affected-says-privacy-body/>.

[37] The Article 29 WP has suggested following definition: Any form of automated processing of personal data, intended to analyze or predict the personality or certain personal aspects relating to a natural person, in particular the analysis and prediction of the person's health, economic situation, performance at work, personal preferences or interests, reliability or behavior, location or movements, <http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2013/20130513_advice-paper-on-profiling_en.pdf>.

[38] Republic of Estonia, Center for Registries and Information Systems, 26.10.2014 <http://www.egov-estonia.eu/>.

profiling by analyzing data with regard to certain characteristics. Thus, for example an alcoholic which has previously received medical treatment (a government service) might have trouble applying for a job at a school as it may be made aware as to the previous drug abuse through accessing data on the government's system. Despite a full rehabilitation the person would be continuously disadvantaged. Many such scenarios can be construed to illustrate the risk vast government data collections can have. An additional concern is the disclosure of such data to private entities which operate for commercial gain, thus could use previous strictly private data for example to evaluate the creditworthiness of an individual.

3.7. *Wireless networks and mobile phones*

The privacy risks present in the internet are to some basic extent known to society at large. However, most people underestimate or are completely unaware of the immense privacy implications mobile phones create. They are the perfect surveillance device as they allow geo-location, the recording of audio and video as well as traffic monitoring.

In particular once a mobile phone signs into a wireless network all traffic will be directed through that network. This allows hackers to show the users any content they would like them to see, such as a fake banking website. Furthermore, it allows a third party to monitor online behavior and even read emails, simply by faking an open wireless network to which the phone automatically connects. Combining this approach with new drone technology thus creating a flying wireless hotspot makes it incredibly easy for third parties to access all mobile phones within a certain radius. In order for this to function the wireless mode of the mobile phones must be turned on. These snoopy drones can then follow any "target" and automatically read out the geo-data of all people passing by and identify where they live.[39]

3.8. *Data of Things*

Increasingly the use of "Data of Things" (DoT) which includes for example all household devices that can create and store data which they share over a common wireless network to improve the lives of the individuals occupying that environment lead to great privacy risks. The more data is collected about a person's characteristics the more predictable a person becomes. Such data is pivotal to companies trying to sell their products without having to spend a vast amount of money on advertisements which might not result in the intended effect of boosting sales. With the data collected from these devices the grocery store around the corner will have your order ready before you even know that your are running out of milk. Currently Amazon is testing this on a much more basic level by trying to anticipate an existing customer's shopping needs and having the products ready to ship even before an order is placed.[40]

Some of the growing privacy concerns can be addressed through appropriate terms of service agreements; others require technological advancements in order to make them safer. Companies should be incentivized to improve their products such as DoT devices and mobile devices by increasing their liability for preventable security breaches which affect the privacy of their customers. Currently the liability in Europe for such breaches due to negligence is low.[41] The US has much stricter product liability laws, however, they also do not yet cater for the threats created by new technology.

4. Technological solutions

In order to achieve the right balance between privacy protection, technological development and entrepreneurial freedom various actions targeted at the individual technology's characteristics are necessary. These include general infrastructure measures such as the routing of data on the internet as well as adjusting settings on each user's computer.

4.1. *Current approaches to network access limitation and tracking*

Currently the ETH in Zurich is developing a new "internet", which will allow the user to determine through which routers the data should be transferred. In doing so a user can avoid countries with inadequate data protection levels or locations from which hacker attacks are to be expected.[42] On first glance this seems to be a sensible approach, however, as such technologies would in essence undermine the integrity and independence of the internet and potentially lead to fragmentation the human rights implication of such measures should also be closely scrutinized. Some authoritarian regimes might have an inherent incentive in limiting access to the internet in order to preserve their form of government. The internet has so far achieved much political advancement which would not have been possible without the ease of access and information dissemination provided by it. Recent examples of its success are the protests in Turkey and some of the North African states.

New technological solutions are being also designed by the advertising industry. For example the Digital Advertising Alliance (DAA) introduced an icon embedded in behaviorally targeted online advertisements which informs the customer of the form of targeting that is conducted as well as any opt out options.[43] One of these options consists in changing browser settings that disallow the tracking of browsing

[39] Motherboard, All The Ways To Hack Your Phone: Phreaked Out (Episode 3), 5.06.2014, <http://www.youtube.com/watch?v=dysnKiXUlRU>.

[40] WSJ, Amazon Wants to Ship Your Package Before You Buy It, 17.01.2014, <http://blogs.wsj.com/digits/2014/01/17/amazon-wants-to-ship-your-package-before-you-buy-it/>.

[41] Rolf H. Weber, Dominic N. Staiger, Cloud Computing: A cluster of complex liability issues, Web Journal of Current Legal Issues, 2014, Vol. 20, No 1.

[42] Andreas Hirstein, ETH-Forscher erfinden das Internet neu, Neue Züricher Zeitung, 01.06.2014, 27.

[43] See Press Release, Interactive Advertising Bureau, Major Marketing/Media Trade Groups Launch Program to Give Consumers Enhanced Control Over Collection and Use of Web Viewing Data for Online Behavioral Advertising (Oct. 4, 2010), <http://www.iab.net/about_the_iab/recent_press_releases/press_release_archive/press_release/pr-100410>.

behavior. Additionally, the DAA has committed itself to ensuring that the information collected will not be used for secondary purposes such as the above mentioned applicant screening or credit decisions.

Further steps are being taken by the World Wide Web Consortium ("W3C")[44] which includes DAA members, industry and consumer groups. The aim of this consortium is to design privacy standards for mobile as well as desktop solutions. Under such a system the user sends a DoNotTrack (DNT) signal via its browser to the site which then applies the tracking in accordance with the user's wishes. So for example when the user has the setting on DNT = 1 no tracking will be allowed.[45] The service provider can then not track the user if it has committed itself to this standard. However, certain permitted use exceptions are included in these standards which do allow the retention of data for specific purposes. These encompass the data to avoid frequency capping (prevent user seeing the same advertisement twice), the data for billing and logging and the data stored for security purposes.[46] Importantly, the user is required to ensure whether his settings comply with his wishes. Nevertheless, in conflicting cases preference should be given to a DoNotTrack signal unless the user has expressly consented to the use of tracking by another unambiguous method.[47]

With respect to geo-location the W3C has released an API Specification addressing some of the dominant privacy concerns. Section 4.1 of the Specification clearly requires the consent of the user before sending the location information to the site. Such consent can be acquired through an interface (as discussed above) or through an established trust relationship with the user.[48] Thus consent must be revocable at any time and the use of the data is limited to its original purpose, requiring deletion upon fulfillment.

4.2. *Privacy Enhancing Technologies*

Privacy Enhancing Technologies (PET) are grouped into four main categories. These include encryption tools, policy tools, filtering tools and anonymity tools. Their aim is to improve user privacy control and to remove unnecessary personal identifiers from communication. (i) As a start encryption software provides a good, cheap basis for protecting one's private communication. In order for the system to work properly all parties must use the same encryption software. (ii) Policy tools such as the ones suggested by W3C allow for automated decision-making when certain privacy settings are applied to the browser's privacy policy on the device. When the other party (the service provider) does not support the privacy policy the browser will block this site or alert the user to its risks. (iii) Filtering tools will complement the privacy policies by blocking unwanted website traffic which is known not to meet minimum privacy standards. (iv) In order to obscure ones identity on the internet anonymity tools which mask the IP address and location of the sender prevent websites and services to determine the location of the user and his identity, hindering to some extent the tracking and profiling capabilities.

Technologies such as .Net Passport protect the privacy of the individual by acting as an intermediary between the customer and the merchant. All the customer data such as name address and bank details are stored in the privacy provider's passport system. The privacy provider is then responsible for sending only the required customer data to the parties involved in the transaction. Thus no party receives more information than it needs. In order for this system to function the merchants must have accepted the passport system and acquire a merchant ID. Nevertheless although the system is very convenient it essentially does lead to the user giving up his ability to control his data.

4.3. *New search engines*

The increased awareness of the amount of monitoring the major search engines such as Google, Bing and Yahoo carry out in regard to their users has lead people to shift their business to other alternatives such as DuckDuckGo. Such search engines allow the user to search online without being monitored and are secured through an encrypted protocol. They do not store searches and minimize privacy intrusion to the level necessary to provide the search service.[49]

As the business models of all search engines are based on advertisement knowledge about the users' interests this knowledge is paramount in order to achieve high profits. Currently the market for search engines is dominated by Google with a global market share of more than 90% in Europe.[50] Changing Google's approach to privacy protection will therefore require regulatory action by states as well as customer pressure. Such pressure can only be achieved if customers demand a better protection of their privacy and are willing to switch to another service which offers such.

Regulators should in particular focus on enforcing customer rights in regard to receiving information on the use of their data as well as their rights to object to such. Furthermore, the mechanisms must enable the users to easily limit the disclosure of their information.

4.4. *Deletion of online data*

In order to "manage" ones online identity, tools need to be in place which allow a person who is affected by a disclosure to

[44] The W3C is an international standard-setting body that works "to lead the World Wide Web to its full potential by developing protocols and guidelines that ensure the long-term growth of the Web." See W3C Mission, <http://www.w3.org/Consortium/mission.html>.

[45] Tracking Compliance and Scope W3C Working Draft, 8 May 2014, <http://www.w3.org/TR/tracking-compliance/#tracking>.

[46] Tracking Compliance and Scope W3C Working Draft, 8 May 2014, Section 5.3. http://www.w3.org/TR/tracking-compliance/#tracking.

[47] Tracking Compliance and Scope W3C Working Draft, 8 May 2014, Section 7, <http://www.w3.org/TR/tracking-compliance/#tracking>.

[48] Geolocation API Specification W3C Recommendation 24 October 2013, <http://www.w3.org/TR/geolocation-API/#security>.

[49] DuckDuckGo, <https://duckduckgo.com/privacy>.

[50] Statista, Worldwide market share of leading search engines from January 2010 to July 2014, <http://www.statista.com/statistics/216573/worldwide-market-share-of-search-engines/>.

have the data deleted or delisted from a search engine. The central issue in such a case is twofold.

4.4.1. *Deleting data links*

Firstly, the individual must have the right to have the data link deleted. Such action might stand in strong contrast to other fundamental rights such as free speech provisions. However, it seems that at least in regard to information found on a governmental source which is subject to a higher level of trust by the public such a right needs to exist. Over time the balance between the interests of the public to have access to certain information shifts in favor of the individual affected. Once his privacy interest outweighs the public interest the individual should be able to enforce his "right to be forgotten".[51]

In Europe this right has been found to exist by the European Court of Justice judgment in Google Inc. v. Agencia Española de Protección de Datos (AEPD).[52] The Court determined that the deletion of an automatic keyword suggestion was appropriate as it implicated the aggrieved party with a foreclosure action which had been carried out against his property more than 10 years ago. As bankruptcy information is only stored for up to 7 years and deleted afterwards, the public access to this foreclosure action clearly was not proportionate anymore.

Secondly, the issue then becomes a technical one as to the ability of various actors in the online world to actually carry out a request for the deletion of the link to the data. Once data is available online it can be copied and duplicated by any party gaining access to it. Although Google for example has the ability to delete specific references to this information upon request, the data can and will be found online at another location which then also requires the deletion of that link. This chain might well become an endless one, unless one could specifically identify the data in question and avoid its referencing already at the time of collection by the search engine. The tools to do this are in place which the effectiveness of censorship technology applied by authoritarian regimes in many parts of the world demonstrate. Nevertheless, the balance must be struck between the individual's right to privacy and the liberties of society such as the freedom of speech. In doing so a speedy, efficient but also objective procedure has to be implemented to allow an aggrieved party to have at least the links to the data removed as a first step in situations in which his right to privacy clearly outweighs public interest.

4.4.2. *Deleting stored data*

Once the links are deleted, one must turn to the actual data itself. Over the last 10 years there has been a lot of discussion within the scientific community on how to achieve a data deletion right. A possible solution would be to incorporate a certificate with the data set created which requires the automatic deletion of the data once a certain time period has elapsed.[53] However, in order to implement such a system the entities storing the data must adhere to such a necessary certification system and encourage its use. As data, whatever its kind, is of immense value to any company because of the possible Big Data analysis that can be conducted with it, such a system is not advocated by the industry. Rather a post factum deletion upon a clear court order is currently the predominant position. The CEO of Google, Eric Schmidt, acknowledged that the "lack of a delete button on the internet is in fact a significant issue".[54] Having such a deletion button would also carry risks because it opens the door for fraudulent behavior as the information used in a crime can be deleted thus preventing or hindering the trace of an individual who committed a crime.

New technological approaches are necessary to empower the user creating a data set for the first time to determine how long the set should be in existence and who can access it. Currently, even deleting an existing customer account is nearly impossible. Most sites do not delete the account but simply deactivate it. Thus the user must manually delete all information on the account, register a new (temporary) email address and then deactivate the account in order to be certain that his personal information is not used anymore (or is of no use to the company). All requests will then be sent to the new email address which is deleted once the account changes have been carried out.

Facebook recently leaked information that it will introduce a system called Slingshot which allows Facebook users to send pictures and text which will delete themselves after a predetermined period of time.[55] Such messaging systems are growing increasingly popular with over 700 million Snapchat messages sent per day.[56] They only function within a proprietary system preventing the user from sending them to another provider. Thus, steps must be taken to enforce a uniform system or standard.

Nevertheless, risks remain when transferring data into the cloud as the recent example of leaked private pictures of various celebrities collected from the Apple iCloud system demonstrated. The risks generally are not based in the terms of the cloud provider allowing a disclosure to third parties but the ability of hackers to obtain the username and password combination necessary to access the files stored in the cloud.[57] Thus, as a rule nobody should store files in the cloud which would cause harm if made public. Sensitive files should

[51] Giovanni Sartor, The right to be forgotten: Publicity, privacy and the passage of time, in: Schartum/Bygrave/Bekken (eds.) Jon Bing A Tribute, 2014, 79–103.

[52] Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González, ECJ C 131/12 <http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=11654>.

[53] Viktor Mayer-Schönberger, delete. The Virtue of Forgetting in the Digital Age, Princeton and Oxford 2009, 178.

[54] Austin Carr, Google's Eric Schmidt On Data Privacy: The Internet Needs A Delete Button, <http://www.fastcompany.com/3009390/tech-forecast/googles-eric-schmidt-on-data-privacy-the-internet-needs-a-delete-button>.

[55] Handelsblatt Online, Facebook lernt vergessen, 10.06.2014, <http://www.handelsblatt.com/technologie/it-tk/it-internet/neue-app-slingshot-facebook-lernt-vergessen/10014844.html>.

[56] Lori Sandoval, Snapchat introduces live video chat, instant messaging. Hello, WhatsApp, Kik, and the gang. 3.05.2014, <http://www.techtimes.com/articles/6409/20140503/snapchat-introduces-live-video-chat-instant-messaging-hello-whatsapp-kick-and-the-gang.htm>.

[57] Apple Media Advisory, 02.09.2014, <http://www.apple.com/pr/library/2014/09/02Apple-Media-Advisory.html>.

be stored locally as this information can only be accessed by placing a trojan software or other spyware on the computer which are detectable by appropriate security software. In order to ensure a high level of safety login information should be regularly changed. A recommended method would be to use a token device creating an alphanumerical code which can be changed regularly. However, because of convenience most users retain the same password for a long duration of time and even use the same password for various services. If necessary this should only be done for non-private and unimportant services which do not store personal or financial information.

5. Outlook

Throughout the debate on protecting privacy the concerned persons and entities realized that there is no one-stop shop solution. Rather a multifaceted approach is necessary encompassing legislative and regulatory measures as well as a change in consumer behavior and market demand for privacy. New frameworks must be developed to cater for the diverse privacy issues created through emerging technologies such as Big Data, cloud computing, mobile services and Data of Things. Privacy protection will also face a growing number of challenges outside the online world such as new drone technologies. First steps have been taken in this regard with Amazon seeking a license to test a new drone type for small parcel delivery.[58] Furthermore, new payment devices are developed such as Bluetooth beacons which allow for the tracking of a customer's buying behavior and pattern recording.[59]

Regulatory measures addressing these issues can either be driven by a bottom-up or top-down approach. In a top-down scenario generally a state's executive organs identify the need for specific regulation which is then enacted by the legislature. However, increasingly the demand for regulation in particular privacy laws is driven by consumers. This bottom-up initiative of the affected individuals demands action from the legislature to ensure protection in regard to specific issues which have arisen from new technologies. It reflects the innovative forms of broad mass participation now being enabled through cloud computing and crowd platforms and it can more easily tackle the problem of the regulatory lag.

In order to address the identified issues new ways of communicating data protection, improved privacy and security standards must be developed and implemented. These standards should be easy to comprehend by simply looking at them. Color-coding could provide an approach which will highlight risk areas (i.e. in red color) and draw attention to them. This would also encourage competition to ensure privacy of the users by allowing the customer to choose the service provider according to the level of privacy required.

It is also imperative that public service agencies ensure that the data they collect and the process of collection is sufficiently protected. As the data is not processed and stored by the agencies themselves but by a subcontractor such as the big IT enterprises (Google, Microsoft) appropriate safety measures must be put in place. These include deletion and retrieval obligations as well as liability for service downtime and data security. One of the first states to contract out public service IT infrastructure to a private enterprise was the City of Los Angeles. It was able to negotiate with Google an increased liability cap of 7.7 million USD for their contracted cloud service demonstrating a change to the prevailing one size fits all approach.[60]

Acknowledgment

The author would like to thank MLaw Dominic N. Staiger (Attorney-at-Law) for his valuable insights and research in preparing this article. A first version of this article has been published under the title "Technological challenges for privacy protection" in: Sylvia Kierkegaard (ed.), Information Ethics and Security – Future of International World Time, Copenhagen 2014, 49–59.

[58] FAZ, Amazon beantragt Testlizenz, 11.07.2014, <http://www.faz.net/aktuell/wirtschaft/netzwirtschaft/amazon-beantragt-drohnen-lizenz-13039724.html>.

[59] Christian A. Goosen, Design and Implementation of a Bluetooth 4.0 LE Infrastructure for Mobile Devices, <http://dbis.eprints.uni-ulm.de/1063/1/BAGoosen_14.pdf>.

[60] City of Los Angeles, Professional Services Contract between the City of Los Angeles and Computer Science Corp. for the SaaS E-Mail and Collaboration Solution (SECS) (2009), <https://sites.google.com/a/lageecs.lacity.org/la-geecs-blog/home/faqs-1/C-116359_c_11-20-09.pdf?attredirects=0&d=1>.