SPRINGER BRIEFS IN CYBERSECURITY

Rolf H. Weber · Ulrike I. Heinrich

Anonymization

Springer

SpringerBriefs in Cybersecurity

For further volumes:
http://www.springer.com/series/10634

Prof. Dr. Rolf H. Weber
Faculty of Law
University of Zurich
Zurich
Switzerland

Ulrike I. Heinrich
Faculty of Law
University of Zurich
Zurich
Switzerland

ISSN 2193-973X
ISSN 2193-9748 (electronic)
ISBN 978-1-4471-4065-8
ISBN 978-1-4471-4066-5 (eBook)
DOI 10.1007/978-1-4471-4066-5
Springer London Heidelberg New York Dordrecht

Library of Congress Control Number: 2012936253

Abstract

Particularly within the last decade the Internet has developed as a phenomenon encompassing social, cultural, economic, and legal facets. Since it has become common practice to use the Internet for both retrieving and providing information it gained the position of a very valuable tool in everyday life. Contrary to many Internet participants' erroneous assumption of surfing on the Internet anonymously, unless disclosing their identity by entering private data, users leave data tracks on each website they pass. Accordingly, surfing on the World Wide Web is far from being an anonymous activity of no consequences. Hence, the decision not to make available personal data best protects the informational and communicative self-determination of the persons concerned since with the development of new technologies new attacking tools are regularly developed, too. For putting the netizens' wish for anonymous communication and the protection of their privacy in the online world into practice, in recent years a number of networking techniques have been innovated. With regard to the fact that these techniques are also misused for illegal activities since parallel to the information and communication technologies' development and the augmented use of the globally available World Wide Web as communication tool crimes and/or their preliminary measures increasingly shift from the real into the online world, on the one hand it is still a debatable point whether there is (or should be) a right to act anonymously on the Internet; on the other hand, governmental interventions into anonymity requests should only be legal if a sufficiently legitimized public interest is given.

Rolf H. Weber—Professor of civil, European and commercial law at the Law Faculty of the University of Zurich, Switzerland, and Visiting Professor at the University of Hong Kong, Kong Kong, attorney-at-law (Zurich).

Ulrike I. Heinrich—Attorney-at-law (Berlin), research assistant and PhD student at the University of Zurich.

Contents

Chapter 1
Notion of Anonymity

1.1 Term and Meaning of Anonymity

Stemming from the Greek word "anonymia", the term anonymity/anonymous stands for "namelessness", "not identified" or "of unknown name" (Oxford Dictionaries) and usually bears on a person's appearance in public. Consequently, anonymity occurs if a person's identity being involved in a not-transparent/not disclosed process is non-determinable since the acting person remains unknown to the other acting entities or makes no appearance towards the other participants or acts within the anonymous process without recognizable name (Bundesamt für Sicherheit in der Informationstechnik 2001, Chap. 1).

However, anonymity does not necessarily presuppose the complete anonymousness of a person's identity or the lack of a name; even the unrenownedness of an individual's name could suffice (Brunst 2009, p. 7). In order to distinguish anonymity from undetectability, it is therefore imperative that one party vaguely knows about the existence of another party without knowing his/her complete identity (Wallace 1999, p. 25).

A further differentiation needs to be made towards pseudonymity which is characterized by the use of a false name even though this practice may lead to anonymity, too. Concerning this issue Froomkin distinguishes between four forms of identification, namely (1) traceable anonymity, (2) untraceable anonymity, (3) traceable pseudonymity and (4) untraceable pseudonymity (Froomkin 1995, para. 11): (1) In the case of communication by email Froomkin refers to traceable anonymity if the receiver of an email gets no information about the identity of the email's originator directly but could find it out by contacting the interconnected operator. (2) Compared with this, in the case of untraceable anonymity, the author of the email is unidentifiable at all. In respect of pseudonymity, Froomkin refers (4) to untraceable pseudonymity if the email's originator uses a false and untraceable identity and, in contrast, assumes (3) traceable pseudonymity if the used pseudonym can be traced back to the originator regardless of whether by the mail's recipient or by someone else.

R. H. Weber and U. I. Heinrich, *Anonymization*, SpringerBriefs in Cybersecurity.
DOI: 10.1007/978-1-4471-4066-5_1, © The Author(s) 2012

1.2 Underlying Motivations of Anonymity

Anonymous actions have a long history and "anonymous pamphlets, leaflets, brochures and even books have played an important role in the progress of mankind" (Solove 2007, p. 139).[1] Hence, the individuals' motivations of making an appearance without revealing their identity are manifold. The intentions range from legal, legitimate and socially approved reasons to a wide range of illegal reasons.

Considerations of staying incognito are understandable for instance in the context of charity acts or for sheltering a person from unwanted contacting or persecution (Solove 2007, p. 139). Insofar, the possibility to act anonymously enables people among others to be more courageous with regard to their expression of opinions. Beyond that anonymous acting opens the chance to be heard free of prejudice or even offers an "identity thief" the opportunity to be heard at all. Not only in the information and communication sector anonymity plays a role; for example in a broader economic context, the French term for the US/UK "stock corporation" is "société anonyme", i.e. the shareholders of the corporation are not known since ownership should not be made known to the public; the participation is evidenced by bearer shares.

The movie "Anonymous" directed by Roland Emmerich and shown to the public in cinemas at the end of 2011 revisits this topic by seizing the conspiracy theory of William Shakespeare not being the originator of his published writings, thus referring to the aforementioned case configuration of pseudonymity. This theory's proponents, the so-called Oxfordians,[2] among others Mark Twain, Henry James and even Sigmund Freud, argue that William Shakespeare who came from a poor background did not possess the education for composing his writings, especially since he was rumored to be an analphabet. According to them, the actor William Shakespeare of Stratford, who has never been on foreign travel, could not possess such a special knowledge to historically correctly write the world-famous tragedies and comedies, as for instance "Henry V", "Othello" or "The Merchant of Venice".

To a great extent, these skeptics were of the opinion that Edward de Vere, the 17th Earl of Oxford, had been the true originator of the writings being published under the name of William Shakespeare. Edward de Vere, a culturally educated man who lived in Venice, Italy, for a while, was told to be a connoisseur of the Elizabethan court culture and a poet. The question of whether William Shakespeare himself or someone else was the originator of the writings published

---

[1] "Persecuted groups and sects from time to time throughout history have been able to criticize oppressive practices and laws either anonymously or not at all.": Talley v. California, 362 U.S. 60 (1960).

[2] Oxfordians are the supporters of the Oxfordian theory of Shakespearean authorship whereby Edward de Vere, 17th Earl of Oxford (1550–1604), wrote the writings traditionally attributed to William Shakespeare.

under the name of William Shakespeare divided the minds for centuries into Stratfordians[3] and Oxfordians even though to date there is no evidence for the defamatory statement of William Shakespeare not being the author of the writings attributed to him (exemplary: Sammartino 1990).

Even though there is a wide range of "good" reasons to stay incognito, the negative aspect of acting without being recognized is not to be underestimated since anonymity places people in the position to act much more unbiased and quite often meaner and less civiled in their speech (Solove 2007, p. 140) which involves the risk to harm other people's reputation. Simultaneously, staying anonymous by taking up another person's identity offers people the possibility of dodging behind a foreign identity and therewith grants the advantage of giving an opinion without bearing possible consequences on one's own behalf.

With the emergence and development of the online world the Internet became a valuable tool in everyday life encompassing social, cultural, economic and legal facets. Associated therewith the communications behavior of people all over the world has also changed; therefore, the particularities of the communication in the offline and the online world, particularly the anonymous communication, are to be addressed subsequently.

1.3 Characteristics of Communication

1.3.1 Real World

The term "real world" describes the "material, physical, atomic and molecular world of everyday human interactions" (Kabay 1998, p. 4). Forms of communication in the real world that indicate a disconnected state like talking on the telephone, writing letters or even talking face to face are referred to as communication in an "offline" world (Weber 2012a).

Communication within the offline/real world is characterized by anonymity (at least to a far extent) (Bizer 2000, pp. 61/62); neither paying a bill in a restaurant or supermarket in cash nor walking in public requires a previous complete announcement of the own identity. Briefly, at first glance the actors' identity is of minor importance within the real world.

Nevertheless, circumstances are different, if the aforementioned payment does not take place by cash but by a financial transaction through electronic payment mechanisms such as money or credit cards (Bizer 2000, p. 62). Within areas like these commercial relations or within personal matters the complete and veritable announcement of a person's identity is regarded as being of importance to guarantee a proper course of the respective procedure. The knowledge of the actors'

[3] Stratfordians are of the opinion that the actor William Shakespeare wrote all the works attributed to him.

identity is of fundamental importance since in case of business relations, assuming the buyer of a good pays with an ec-card, the buyer "just" promises the payment towards the seller. Insofar, the seller can prove a legitimate interest in the real identity of his business partner to protect him financially.

1.3.2 Particularities of the Online World

In addition to the long-known and omnipresent real world a parallel "environment", the so called virtual/online world (Internet), emerged within the last 30 years. In the course of the Internet's development and the increasing public acceptance communication to a great extent shifted into the virtual world and accordingly the issue of acting anonymously emerged there again.

1.3.2.1 Development of the Online World

Dating back to the late 1960s when U.S. researchers first developed protocols that allowed the sending and receiving of messages by use of computers,[4] the term "online" world was coined, referring to communicating via networked computers (Warschauer 2008, p. 207). In the course of the development and the spread of personal computers from the 1980s onwards communication via the Internet, online communication, started to become available to the public at large. Therewith, the percentage of people having Internet access and using web-based systems for the search and purchase of products or the cultivation of contacts has grown vastly since civil society has begun to replace traditional face-to-face communication by using e-services (Van Dijk et al. 2007, p. 7).

By now, working without Internet access is almost inconceivable, at least in developed countries. Rather, the medium Internet became so important for the societal communication that the participation of all is a substantial political task (Holznagel and Schumacher 2011, p. 14). Hence, the question arises of how to maintain all the benefits of the Internet while restricting antisocial communication and acting on the Internet (Kabay 1998, p. 2).

Being originally developed beyond a regulatory legal framework and mainly based on self-regulation by its users, initially the assumption prevailed that cyberspace was an independent new "province" and a legal vacuum in the world (Weber 2009, pp. 3–5 for further details). Thereby and with regard to the fact, that the Internet started as a communication platform of a comparatively small research and academic community (Weber and Schneider 2009, p. 18), the participants' identification within the World Wide Web played a minor role.

[4] The text of this subchapter is partly based on Weber 2012a.

In the course of time, the Internet established itself in everyday life (Demut and Rieke 2000, p. 38). Therewith, especially in view of to the developing electronic commerce, the participants' identifiability and traceability became of concern; just like within the offline world all parties to a contract have a clear interest in knowing their counterpart and obtaining information as for instance about solvency or credibility of further trade partners before concluding agreements.

However, as set out above, there is an interest of a wide range of (Internet) participants to partially stay incognito or even untraceable on the Internet, be it to prevent identity theft, to protect search histories from public disclosure, to get access to all websites or to avoid criminal prosecution.[5] Beyond the legal motivations some Internet users also seek for anonymously acting online to conduct fraudulent financial transactions or launch attacks with little risk of being located by law enforcement agencies and therewith aim at avoiding the consequences of a preceded or scheduled engagement in criminal or socially unacceptable behaviour. With commenters being given the possibility to hide behind a cloak of anonymity, the blog and Internet fora have become places for hatred, discrimination and bile (Adams 2011). Accordingly, the advantages and disadvantages of anonymous acting apply to both, anonymity in the real world ("offline") and in cyberspace ("online").

1.3.2.2 Surveillance and Identification of Internet Participants

(1) Subscriber Identification without the Internet Users' Knowledge

(a) Data Tracks

During the last twenty years Internet participants developed new ways for making use of the World Wide Web; thereby, it has become common practice to use the Internet for both retrieving and providing information (Taddicken 2012, p. 255). In order to be present on the Internet for private or professional purposes, an individual or an enterprise needs to have a specific address, an Internet Protocol (IP) address.[6] IP addresses are not physical and not directly controllable by the

[5] A relevant example in connection with anonymous acting online is the whistle-blowing Internet platform Wikileaks providing capacity for anonymously publishing submissions of private, secret, and classified media thereby following their goal of bringing "important news and information to the public" (http://wikileaks.org/About.html). Having released a number of significant documents in the past the entity sees itself as assistance to peoples of all countries who wish to reveal unethical behaviour in their governments and institutions.

[6] The Internet uses IP addresses to identify computers. Their addresses and names (then called host names) were initially stored on a centralized and monolithic file maintained by the Stanford Research International Network Information Center (SRI-NIC) on their NIC name server. By 1984, these addresses had become very complicated to use. That led people to translate these numbers into words and to organize them in the generic domains by the Domain Name System (DNS); for further details see Weber and Schneider 2009, pp. 19–21.

user since the allocation is (directly or indirectly) derived from Internet Address Registries.

The pool of IP addresses is managed by the Internet Assigned Numbers Authority (IANA),[7] which has since the early 1990s delegated the allocation of Internet resources to five established Regional Internet Registries (RIR) (Edelmann 2009, p. 3; Brunst 2009, pp. 51–53) that are obliged to take due regard to global addressing policies (Lehr et al. 2008, p. 9).[8] These non-profit RIR corporations[9] oversee the allocation of IP addresses to Internet Service Providers (ISP), National Internet Registries (NIR) and individual network institutions; these organisations in turn allocate IP addresses to the individual Internet users. Comparable to a piece of land in the real world, the establishment of a domain name traces out a "territory in cyberspace" which enables communication. To function properly IP address blocks can only be used by one network so as not to lead to conflicts in routing.

Many Internet users still believe in the anonymity of the Internet and the protection of their personal data as long as they do not disclose their identity by entering their name, private address or banking information (Pfitzmann 2000, p. 12; Solove and Schwartz 2011, p. 590; Schwartz and Solove 2011, p. 1837). This assumption is supported by the possibility to send emails or postal messages to electronic bulletin boards under pseudonyms (Solove and Schwartz 2011, p. 590).

In contrast, while surfing on the Internet every computer communicates by using a traceable IP address[10] and therewith leaves a data track on each passed website, meaning the website visited (Solove 2007, p. 147; Landau 2010, p. 139); website log files contain the user's IP address, the time he/she was online and any information the user entered into a webpage or pages the user downloaded (Solove and Schwartz 2011, p. 590). Beyond that, also each mobile phone or other device

---

[7] In 1989, the US Department of Commerce concluded a contract with the Department of Post and Telecommunications' Information Science Institute at the University of Southern California, establishing the Internet Assigned Numbers Association (IANA). Although IANA's tasks were transferred to a great extent to the Internet Corporation for Assigned Names and Numbers (ICANN), IANA among other things is still responsible for the global coordination of the Internet Protocol addressing system allocating IP addresses from the pools of unallocated addresses to the Regional Internet Registries (RIR) according to their needs; for further details see Weber and Heinrich 2011, pp. 78–80.

[8] At the beginning of the Internet, a single authority combined both service areas and distributed the information through the RFC series.

[9] At the present time there are five RIRs in operation, namely the American Registry for Internet Numbers (ARIN) for North America and Parts of the Caribbean, the RIPE Network Coordination Centre (RIPE NCC) for Europe, the Middle East and Central Asia, the Asia-Pacific Network Information Centre (APNIC) for Asia and the Pacific region, the Latin American and Caribbean Internet Addresses Registry (LACNIC) for Latin America and Parts of the Caribbean Region and the African Network Information Centre (AfriNIC) for Africa.

[10] That is why Internet users intending to visit a company webpage will mostly be redirected to the respective country page although having entered another top-level domain; businesses use this automatic onward transfer for selling products in different countries at different prices.

used to access the Internet has a unique IP address and can therewith potentially be traced (European Parliament 2010, p. 42). Accordingly, Internet Service Provider (ISP) (and any eavesdropper on the Internet connection) can monitor the steps users made on the Internet[11]; beyond that ISP have information to link an Internet user's screen name[12] with his/her real identity (Solove and Schwartz 2011, p. 591).

(b) Cookies and Other Applications

Each time the user visits a website also "Internet cookies" are downloaded into the user's electronic device tagging the user with an identification number; these identification numbers can include references to a wealth of information about the user (Solove and Schwartz 2011, p. 590). Internet cookies are small pieces of information in text format that are downloaded to the computer when the user visits a website (European Parliament 2010, p. 43). They may come from the page itself or from the providers of the advertising banners or other graphics that make up a website (Moore 2011, p. 233) and enable computers to remember a user's history on a particular website (Shah and Kesan 2004, pp. 13–17).[13]

A further possibility to identify Internet users by collecting information about them are so-called "web bugs". This technical device also known as "clear graphics interchange format (GIF)" (Nichols 2001, p. 1) is a graphic on a web page or inserted into an email created for the purpose of online tracking. The web bug enables the creator to determine who is reading a web page or email, when, how often, and from what computer. After the recipient opens the email the graphic shall be downloaded from the server eventually at least providing information about the used computer's IP address and the time of the request (Brunst 2009, p. 78). Initially developed in order to enable service providers to tailor services to meet Internet users' needs, the fact of people not recognizing this hidden monitoring makes these programs that dangerous since the tools can be used to monitor Internet users in case of legal and illegal activities (European Parliament 2010, p. 43).

(2) Self-imposed Subscriber Identification

In addition to the automatic collection of data many Internet participants still act very carelessly in dealing with the Internet and the protection of their own privacy. Even though they ascribe high importance to privacy (Barnes 2006), a large percentage of the user community is willing to share personal information under certain circumstances and frequently makes personal information available to third

[11] The announcement of the IP address is essential for enabling their locating by the respective web page operator and for knowing where to "send" the requested information to.

[12] The pseudonym he/she is appearing with on the Internet.

[13] "Cookies" are strings of data introduced by the company Netscape whereby the name was a term already in use in computer science for describing a piece of data held by an intermediary.

parties or allows them to store their personal or non-personal data. This careless behaviour with private data has the potential to lead to privacy and surveillance problems since a user's identity can be achieved by analyzing a "trail of seemingly anonymous and homogenous data left across different locations" (Malin et al. 2003, p. 1).

Several studies have shown that Internet participants in principle provide personal information on websites after request. As already outlined by a 2000 study, 54% of the polled Internet users have chosen to disclose personal information for using a website and an additional 10% would be willing to do this under the right circumstances; only a fourth of the persons asked would never provide personal information (Fox 2000, p. 2).

Furthermore, the dissemination of personal data is actively pursued by the constantly rising frequentation of social networks like Facebook or Myspace[14] and the therein offered possibility to present and position personal information by publishing pictures or giving details about the own private and professional life. According to a 2010 study by Ofcom, the government-approved regulatory authority for the broadcasting and telecommunication industries in the United Kingdom, 33% of the interviewees love putting private photos online, rising to 57% of those aged 16–24 (Ofcom 2010, p. 3). Even though 74% of the interviewed Europeans see disclosing personal information as an increasing part of modern life, only 26% of social network users feel in complete control of their personal data (European Commission 2011b, pp. 2, 22).

This acting very often enables or at least simplifies the Internet participant's identification. Even though the information disclosed should be available to the respective (identifiable) party only, the confidentiality or further transfer of these announced personal data is no longer subject to control by the respective Internet user.

Besides these aspects, with the progress of technical development the growing importance of Internet search engines contributes to the dissemination of data. Once online available data have been indexed by search engines, they can hardly be removed anymore from the World Wide Web. Hence, with the increased tendency to make information of all kinds public, privacy is at risk. Bearing in mind that the online world seems to be full of people willing to share personal information with others it may be easy to forget that there are many users who want to remain anonymous on the Internet (Glater 2006), especially as 70% of Europeans are concerned that their personal data held by enterprises may be used for purposes other than agreed at the time of collection (European Commission 2011b, p. 2).

[14] Social structures such as social networking sites, blogs and wikis made up for individuals (or organisations) that offer possibilities for participation and collaboration.

References

Adams T (2011) How the Internet created an age of rage. The Guardian. 24 July 2011. http://www.guardian.co.uk/technology/2011/jul/24/internet-anonymity-trolling-tim-adams. Accessed 31 Jan 2012

Barnes SB (2006) A privacy paradox: Social Networking in the United States. First Monday 11(9). http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/1394/1312. Accessed 31 Jan 2012

Bizer J (2000) Recht auf Anonymität—ein Rechtsprinzip der elektronischen Individualkommunikation. In: Sokol B (ed) Datenschutz und Anonymität. Toennes Satz + Druck GmbH, Düsseldorf. https://www.ldi.nrw.de/mainmenu_Service/submenu_Tagungsbaende/Inhalt/2000_Datenschutz_und_Anonymitaet/Datenschutz_und_Anonymitaet.pdf. Accessed 31 Jan 2012

Brunst PW (2009) Anonymität im Internet—rechtliche und tatsächliche Rahmenbedingungen. Duncker and Humblot, Berlin

Bundesamt für Sicherheit in der Informationstechnik (2001) Das Ende der Anonymität? Datenspuren in modernen Netzen. https://www.bsi.bund.de/ContentBSI/Publikationen/Studien/anonym/wasistanonymitaet.html;jsessionid=97B15124E289CE809BB8CA90471E5F9A.2_cid241. Accessed 31 Jan 2012

Demut T, Rieke A (2000) Der Rewebber—Anonymität im World Wide Web. In: Sokol B (ed) Datenschutz und Anonymität. Toennes Satz + Druck GmbH, Düsseldorf

Edelmann, B (2009) Running out of numbers: scarcity of ip addresses and what to do about it. Working Paper Harvard Business School. http://www.hbs.edu/research/pdf/09-091.pdf. Accessed 31 Jan 2012

European Commission (2011b) Special eurobarometer 359: attitudes on data protection and electronic identity in the European union. Report. June 2011. http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf. Accessed 31 Jan 2012

European Parliament (2010) Information and communication technologies and human rights. http://www.europarl.europa.eu/committees/en/studiesdownload.html?languageDocument=EN&file=31731. Accessed 31 Jan 2012

Fox S (2000) Trust and privacy online: why americans want to rewrite the rules. The Pew Internet and American Life Project. http://www.pewinternet.org/~/media//Files/Reports/2000/PIP_Trust_Privacy_Report.pdf.pdf. Accessed 31 Jan 2012

Froomkin AM (1995) Anonymity and Its enmities. Journal of Online Law. http://articles.umlaw.net/froomkin/Anonymity_Enmities.htm. Accessed 31 Jan 2012

Glater JD (2006) Privacy for People Who Don't Show Their Navels. The New York Times. 26 January 2006. http://www.nytimes.com/2006/01/25/technology/techspecial2/25privacy.html. Accessed 31 Jan 2012

Holznagel B, Schumacher P (2011) Die Freiheit der Internetdienste. In: Kleinwächter W (ed) Grundrecht Internetfreiheit. Eurocaribe Druck Hamburg, Berlin

Kabay ME (1998) Anonymity and pseudonymity in cyberspace: deindividuation, incivility and lawlessness versus freedom and privacy. http://www.mekabay.com/overviews/anonpseudo.pdf. Accessed 31 Jan 2012

Landau S (2010) Surveillance or Security? The risks posed by new wiretapping technologies. The MIT Press, Cambridge and London

Lehr W, Vest T, Lear E (2008) Running on empty: the challenge of managing Internet addresses. http://cfp.mit.edu/publications/CFP_Papers/Lehr%20Lear%20Vest%20TPRC08%20Internet%20Address%20Running%20on%20Empty.pdf. Accessed 31 Jan 2012

Malin B, Sweeney L, Newton E (2003) Trail re-identification: learning who you are from where you have been. LIDAP-WP12. Carnegie Mellon University. Laboratory for International Data Privacy. http://dataprivacylab.org/dataprivacy/projects/trails/paper3.pdf. Accessed 31 Jan 2012

Moore R (2011) Cybercrime: investigating high-technology computer crime, 2nd edn. Anderson Publishing, Burlington

Nichols S (2001) Big Brother is Watching: An update on web bugs. http://www.sans.org/reading_room/whitepapers/threats/big-brother-watching-update-web-bugs_445. Accessed 31 Jan 2012

Ofcom (2010) Media Literacy Matters, Online trust and privacy: People's attitudes and behaviour. Research Document. http://stakeholders.ofcom.org.uk/binaries/research/media-literacy/trust-privacy.pdf. Accessed 31 Jan 2012

Pfitzmann A (2000) Möglichkeiten und Grenzen von Anonymität. In: Sokol B (ed) Datenschutz und Anonymität. Toennes Satz + Druck GmbH, Düsseldorf

Sammartino P (1990) The man who was William Shakespeare. Cornwall Books, New York

Schwartz PM, Solove DJ (2011) The PII problem: privacy and a new concept of personally identifiable information. New York Univ Law Rev 86(6):1814–1894

Shah RC, Kesan JP (2004) Recipes for cookies: how institutions shape communication technologies. http://www.governingwithcode.org/journal_articles/pdf/Recipe_For_Cookies.pdf. Accessed 31 Jan 2012

Solove DJ (2007) The future of reputation: gossip, rumor, and privacy on the internet. Yale University Press, New Haven

Solove DJ, Schwartz PM (2011) Information Privacy Law, 4th edn. Wolters Kluwer Law, New York

Taddicken M (2012) Privacy, surveillance, and self-disclosure in the social web: exploring the user's perspective via focus groups. In: Fuchs C, Boersma K, Albrechtslund A, Sandoval M (eds) Internet and Surveillance: The Challenges of Web 2.0 and Social Media. Routledge, New York

Van Dijk G, Minocha S, Laing A (2007) Consumer, channels and communication: online and offline communication in serve consumption. Interact Comput 19:7–19

Wallace KA (1999) Anonymity. Ethics Inf Technol 1(1):23–35

Warschauer M (2008) Online communication. In: Carter R, Nunan D (eds) The Cambridge guide to teaching english to speakers of other languages. Cambridge University Press, Cambridge

Weber RH (2009) Internet governance: regulatory challenges. Schulthess, Zurich

Weber RH (2012a) International governance in a new media environment. In: Price ME, Verhulst SA (eds) Handbook of media law and policy: a socio-legal exploration. Routledge, New York (forthcoming)

Weber RH, Heinrich UI (2011) IP Address allocation through the lenses of public goods and scarce resources theories. scripted 8(1): 69–92. http://www.law.ed.ac.uk/ahrc/script-ed/vol8-1/weber.pdf. Accessed 31 Jan 2012

Weber RH, Schneider T (2009) Internet governance and Switzerland's particular role in its processes. Schulthess, Zurich

Chapter 2
Anonymity Challenges in the Internet

Since information about people acting in the Internet (both, consciously or unconsciously provided by them) can be easily found, surfing on the World Wide Web is far from an anonymous activity of no consequences. With regard to the therewith associated risk of data abuses it is still a debatable point, whether the identification in the online world is essential, and if so to what extent, or whether there is a right to act anonymously within the World Wide Web.

In this sense, light will subsequently be shed on the motivations for the anonymous use of Internet services and the Internet participants' possibilities to make their activities on the Internet untraceable.

2.1 Risks for Anonymous Use of Internet Services

Manifold Internet activities cause risks for those persons being interested to remain anonymous when using the new communication channels and platforms. Some practices leading to data collection and consequently to the possibility of third persons to have access to personal data are discussed hereinafter.

2.1.1 Information Gathered by IP Addresses

Internet IP addresses[1] are used to route data from one host computer to another. Even though these numerical addresses do not directly identify particular Internet users, their identification can easily follow from the connected addresses by evaluating the gathered information (Schwartz and Solove 2011, pp. 1838/1839).

Initially, static IP addresses were used. A static IP address is a number (in the form of a dotted quad) that is assigned to a computer by an Internet Service

[1] See Sect. 1.3.2.2(1)(a).

R. H. Weber and U. I. Heinrich, *Anonymization*, SpringerBriefs in Cybersecurity,
DOI: 10.1007/978-1-4471-4066-5_2, © The Author(s) 2012