Chapter 4
Limitations of Anonymization

4.1 Factual Reasons for State Interventions

As previously mentioned, the Internet users' intentions to stay anonymous in the Internet are manifold and range from legal to a wide range of illegal reasons. Proponents of a right to stay anonymous on the Internet mainly rest their position on the protection of the individual's data and on privacy[1]; the opposing side calls for a transparent Internet enabling no anonymous acting on the Internet. For consolidating their positions the advocates of transparency refer to the ongoing violations of rights committed by Internet users curtaining their identity and therewith seeking for abdicating responsibility.

Recently, especially subsequently to the tragic events in Norway in summer 2011, voices were again being raised to completely stop anonymous acting on the Internet. On 22 July 2011 a Norwegian right-wing extremist accomplished two sequential terrorist attacks previously announced online with 77 people killed and many people injured; over a period of years prior to his attacks the Norwegian extremist had participated in Internet for a debating against immigration and the Islam and published a hate-filled manifesto by appearing on the scene anonymously, just using a pseudonym.[2]

Additionally, iterative hacker attacks of Internet users contribute to the revivification of the debate concerning the justification of a right to stay anonymous on the Internet. Within the last months repeatedly hacker attacks by individuals or groups hiding their IP addresses by using anonymizing services like proxy servers[3] acting among others under the pseudonym "Anonymous"[4] were reported pursuing

[1] See Chap. 3.
[2] Pseudonymity is characterized by the use of a false name and for the most part eventuates in anonymity; see Sect. 1.1.
[3] See Sect. 2.2.2.1(1).
[4] See Chap. 2, footnote 6.

R. H. Weber and U. I. Heinrich, *Anonymization*, SpringerBriefs in Cybersecurity,
DOI: 10.1007/978-1-4471-4066-5_4, © The Author(s) 2012

the objection of illegally penetrating large companies' data bases and spy out customer data or solely to harm companies by immobilizing their web pages.[5]

Hence, national policy and State security organisations have to also focus their attention to the actions taken within the virtual world, at least since the number of terrorist incidents has increased starting with the attacks of 11 September 2001 against the United States of America. During these devastating attacks terrorists hijacked four US passenger jets and misused them for conducting suicide outrages; thereby more than 3,000 people lost their life. The terrorists directed two passenger jets into the towers of the World Trade Centre in New York and the third one into the Pentagon in Arlington, Virginia; the fourth passenger jet was programmed to hit a government building in Washington D.C. but crashed earlier because of fights between hijacksers and passengers. In the forefront of the attacks the terrorists among others connected and communicated by (mis)using the anonymity of the Internet.

As a result of the attacks, governments all over the world enacted regulations to combat terrorism, partially including the authority to monitor telephone communications, email, and Internet use of terror suspects. Governments vindicate these measures with the fulfillment of their superordinate task of protecting their citizens and therewith acting in the public interest. Hence, this duty to protect its citizens and defeating offences is confronted with the individual's interest on privacy, as in the case of an acting anonymously on the Internet.

Since not all possible limitations of anonymity can be addressed, the following subchapters particularly shed light on State supervision in general, the combat of cybercrime, the supervision of Internet traffic by Trojan horse software and the enforcement of Internet copyright infringements as special case of illegal Internet activity.

4.2 State Supervision in the Public Interest in General

Generally looking, States do have an interest that the Internet is not used for illegal purposes. The respective risk is imminent since the Internet allows an individual quite easily to remain anonymous; as outlined, anonymity cannot anymore be protected if higher ranking objectives of a State require disclosure of information and transparency.

4.2.1 Legitimate State Interests

Several interests that can be invoked by States for interventions into the Internet traffic are legitimate. Indeed, the Internet is not a sphere being outside of the scope

[5] See exemplary attacks of "Anonymous" vs. Stratfor, Sect. 2.1.3.

of the legal framework at all. The proclamation of John Perry Barlow in his manifesto "A Declaration of the Independence of Cyberspace" of 1996 containing the sentence "You [governments] have no moral right to rule us, nor do you possess any methods of enforcement we have true reason to fear" (Barlow 1996) has obviously turned out to be wrong. Early legal scholars also assessed the legal situation in an improper way: "There is no regulatory body, and computers are capable of anything.[…] Since there is no regulatory body policing the Internet, the extent to which an individual is capable of speaking without restriction is an enigma" (Ryga 1995, pp. 221, 223).

The most obvious example for a legitimate state intervention is the interest of combating cybercrime.[6] Other reasons could be the realization of public order and public morals or the enforcement of property rights.[7]

Public order and public morals obviously depend on the given circumstances and the national appreciation of State interests. Therefore, a globally accepted definition of these terms is not available. Nevertheless, the WTO-law knows these terms, namely in Art. XX of the GATT (only public morals) and Art. XIV of the GATS (public order and public morals). In the field of the delivery of cross-border services, the dispute settlement bodies of the WTO have assessed these terms in two cases, namely the "US- Gambling case" and the "China—Publications and Audiovisual Products case":

- Public order "refers to the preservation of the fundamental interests of a society, as reflected in public policy and law. These fundamental interests can relate, inter alia, to standards of law, security and morality".[8] The focus is on societal interests, similar to those in international private law like fundamental values and concerns of the country's society (Cottier Delimatsis and Diebold 2008, p. 299, margin number 22).
- Public morals refer to "standards of right and wrong conduct maintained by or on behalf of a community or nation".[9] Public morals are influenced by each country's prevailing social, cultural, ethical and religious values.[10] Legal doctrine interprets "public morals" as encompassing measures relating to alcohol, sex, gambling, slavery, torture of animals and drugs (Cottier Delimatsis and Diebold 2008, p. 298, margin number 21).

---

[6] See Sect. 4.3.

[7] See Sect. 4.5.

[8] United States—Measures affecting the cross-border supply of gambling and betting services (US—Gambling), WT/DS285/R, Panel Report, para 6.467.

[9] Id. para 6.465.

[10] China—Measures affecting trading rights and distribution services for certain publications and audiovisual entertainment products, WT/DS363/R, Panel Report, para 7.763.

Notwithstanding the fact that the two terms stand for two distinct concepts, some overlap exists; both terms seek to protect similar values.[11] Partly it is argued that public order is broader than public morals since it includes further interests such as safety and access to essential facilities (Munin 2010, p. 357). In the context of the anonymity assessment, however, the details of the relationship between public order and public morals (see for further details Cottier Delimatsis and Diebold 2008, p. 299) does not need to be elaborated further; moreover, the interpretation in the given situation of a State intervention as well as the fulfillment of general legal principles such as the necessity, proportionality and suitability of the measure are decisive.

Furthermore, international legal instruments regularly contain clauses allowing States to limit the exercise of fundamental rights; examples are

- Article 19 para 3 ICCPR (United Nations 1966) stating that "the exercise of the rights provided for in paragraph 2 of this article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary: (a) For respect of the rights or reputations of others; (b) For the protection of national security or of public order (ordre public), or of public health or morals."
- Article 8 para 2 ECHR (Council of Europe 1950)[12] stating that "there shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others".

Summarizing, legitimate State interests can exist, justifying governmental intervention into the sphere of anonymization of individuals. As international legal instruments, however, show in different ways and in not identical words, the public order argument can only be legitimately invoked if a fundamental interest of a State calls for a specific measure. The respective rules, allowing interventions, must be interpreted in a narrow way in order to ensure that the individual protection regime will not be undermined over time.

4.2.2 Legal Bases for State Interventions

4.2.2.1 Determination of Scope of Human Rights

State interventions into the Internet traffic jeopardize the exercise of human rights. The most important rights are the freedom of expression and the right to privacy.

[11] US—Gambling, supra note 9, para 6.468.

[12] See Sect. 3.1.3.1.

The mentioned two human rights themselves can come into a direct conflict since an unlimited freedom of expression most likely interferes with privacy interests and an unlimited right to privacy makes the free exchange of communication in the Internet hardly possible.[13]

The new Internet age also calls for the development of new fundamental rights which are suitable to more precisely deal with the particularities of the most recent communication channels. In fact, this way has been chosen by the German Federal Constitutional Court having designed and accepted a so-called "computer confidentiality and integrity right" (German Federal Constitutional Court 2008) within its ruling of February 27, 2008.

The constitutional complaints in question[14] were both based on the doubted constitutionality of regulations of a regional Protection of the Constitution Act (in particular, Article 5 para 2 No. 11 Protection of the Constitution Act of North Rhine-Westphalia) authorizing public authorities (for the protection of the constitution) to secretly monitoring the Internet and, beyond that, secretly accessing information technology systems and thus realizing an online surveillance[15] of suspects. Within its ruling the German Federal Constitutional Court declared the confidentiality and integrity of personal data in information technology systems (private computers, smart phones, etc.) of being a fundamental right comparable to the inviolability of the home (German Federal Constitutional Court 2008: guiding principle No. 1; Rosenbach Stark and Winter 2011) and ruled the secret infiltration of these systems of being an infringement of the general personality right (German Federal Constitutional Court 2008: Sect. 166).

For being constitutionally legitimate, the secret infiltration presupposes circumstantial evidence of the existence of a concrete danger to a legally protected interest of outstanding importance, namely a person's life, limb and freedom, or goods of the community whose menace concern theSstate's fundamentals/existence or the existence of mankind (German Federal Constitutional Court 2008: guiding principle No. 2). However, according to the judgement the secret reconnaissance requires a court order to protect the suspect's "core area of private way of life"; the court order must be based on a law containing precautionary measures to protect the aforementioned core area (German Federal Constitutional Court 2008: guiding principle No. 3).

As outlined, the mentioned international legal instruments know quite similar conditions that must be met in order to make a state intervention legitimate.

---

[13] See Chap. 3.

[14] The group of appellants consists of a journalist, an active politician and two associates of a law firm (German Federal Constitutional Court 2008: Sects. 116–118) who blamed a personality right violation, precisely a violation of the fundamental right in confidentiality and integrity of information technology systems, also referred to as "right to online privacy" or "computer confidentiality and integrity right" (Weber 2011a, p. 128); for an evaluation of this decision see Weber 2008, pp. 94–97.

[15] See Chap. 3, footnote 8.

4.2.2.2 Conditions for State Interventions

A first condition for a State intervention is regularly the formal requirement of having a law in place. Police authorities, for instance in a envisaged criminal prosecution, are not entitled to break into a privacy or anonymity right if the respective action cannot be based on a law formally enacted. Usually, the law has been passed by the parliament, a governmental ordinance is not sufficient. Furthermore, the law must describe with sufficient clarity under which circumstances a state intervention is legitimate.[16] Obviously, the assessment of the quality of law depends on the national legislator; in addition, the lack of a law might be remedied by the enactment of a new legal provision.

A second condition of substantive nature addresses the necessity of the State intervention: The chosen governmental activity has to be proportionate to the envisaged objective of the intervention. Consequently, the measure should not exceed the required limitation of an individual's human right; a balance of interests test (Jackson 2011: 21.029) has to be applied evaluating the corresponding motivations and expectations of the concerned persons/entities.[17]

A third condition concerns the suitability of a governmental measure, thereby including a procedural element: The intervention of the State must be appropriate in view of the envisaged objective being suitable to achieve it in the best possible manner.[18] The European Court of Human Rights refers to "pressing social needs"[19] in the interpretation of the proportionality and the suitability principle.

In addition, the general interpretation principle applies that limitations and restrictions related to the exercise of human rights are to be interpreted in a narrow way, i.e. the legitimacy of state interventions based on the necessity test (proportionality and suitability criteria) must be submitted to a strong assessment[20] of the fulfillment of its conditions.[21]

Recently, a further aspect related to the scope of human rights has been more intensively debated, namely the question whether and, if yes, to what extent human rights have a (minimal) core protection which cannot be touched and limited at all.

---

[16] ECHR: Autronic AG vs. Switzerland, judgment of 22 May 1990, No. 17/1989/175/231, § 57; Rekvényi vs. Hungary, judgment of 20 May 1999, No. 25390/94, § 34.

[17] ECHR, The Sunday Times I vs. The United Kingdom (Series A No. 30), judgment of 26 April 1979, §§ 54 ss.

[18] ECHR: Handyside vs. The United Kingdom, judgment of 7 June 1976, No. 5493/72, § 46; The Sunday Times I vs. United Kingdom (Series A No 30), judgment of 26 April 1979, § 59; The Observer and Guardian vs. The United Kingdom, judgment of 26 November 1991, No. 13585/88, § 59; Krone Verlag GmbH & Co. KG vs. Asustria, judgment of 26 February 2002, No. 34315/96, § 34.

[19] ECHR, Dichand and Others vs. Austria, judgment of 26 February 2002, No. 29271/95, § 1.

[20] ECHR: The Observer and Guardian vs. The United Kingdom, judgment of 26 November 1991, No. 13585/88, § 59; Thoma vs. Luxembourg, judgment of 29 March 2001, No. 38432/97, § 43; Perna vs. Italy, judgment of 25 July 2001, No. 48898/99, § 38.

[21] Non-consensual "searches" of a person are illegal unless authorized by law, i.e. by legislation or as a matter of common law, comp. Jackson 2011: 21.082.

In fact, some Constitutions (for example Germany, Art. 19 para 2 of the Basic Law, or Switzerland, Art. 36 para 4 of the Constitution) know the principle of a core protection of some human rights (see Schefer 2001). State (and private) interventions into this core protection are illegal and can be challenged. For obvious reasons, the scope of the core protection depends on the given societal perceptions of the concerned State. In practical terms, a law forbidding any communication in an anonymous way might not be compliant with the human right to privacy.

Similar concepts can also be derived from international legal instruments: According to the Human Rights Committee, interpreting the International Covenant on Civil and Political Rights of 1966, reasons of public interest "may never be invoked as a justification for the muzzling of any advocacy of multi-party democracy, democratic tenets and human rights".[22] The European Court of Human Rights also stated that a minimal scope of human rights would be inherent to a democracy and interference into such scope would not be justified by pressing social needs (Wildhaber and Breitenmoser 1992: margin number 729). Looking at State interventions into the free flow of traffic in the Internet it seems to be worth to look more closely into the possibility of applying the described core protection concept in the future.

4.2.2.3 Positive Obligations of States

During the last few years the question has been more intensively debated whether States would have so-called positive obligations to actually guarantee the possibility for individuals to fully realize the human rights. The purpose of such an understanding consists in the objective to avoid interference into human rights by private actors. As far as the right to privacy and to confidentiality is concerned, the European Court of Human Rights (ECHR) has approved and requested the existence of positive obligations in several court decisions.[23]

In particular, the ECHR stated under the heading of "general principles" in a decision rendered in 2003[24]: "Effective exercise of this freedom does not depend merely on the State's duty not to interfere, but may require positive measures of protection, even in the sphere of relations between individuals". Furthermore, the

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

[23] ECHR: Kegan vs. Irland, judgment of 26 May 1994, No. 16969/90, § 49; McGinley and Egan vs. The United Kingdom, judgment of 9 June 1998, No. 10/1997/794/995–996, § 98; Guerra and Others vs. Italy, judgment of 19 February 1998, No. 14967/89, § 58; Christine Goodwin vs. The United Kingdom, judgment of 11 July 2002, No. 28957/95, §§ 71/2; compare also Weber and Sommerhalder 2007, p. 97.

[24] ECHR, Appleby and Others vs. The United Kingdom, judgment of 6 May 2003, No. 44306/98, § 39/40.

ECHR held[25]: "In determining whether or not a positive obligation exists, regard must be had to the fair balance that has to be struck between the general interest of the community and the interests of the individual".

An interest of having the State intervening if an individual limits the exercise of a human right of another individual is particularly given of the restrictive activity cannot be based on legitimate reasons: If an Internet Service Provider permanently violates privacy rights of customers, an adequate interest balancing test would have to cause the State to intervene and prohibit the activity of the ISP not complying with privacy principles.

4.3 Combating Cybercrime

4.3.1 Subject Matter of Protection

As mentioned the World Wide Web offers manifold information and communication possibilities which are not necessarily compliant with the addressed (controversial) right to act anonymously therein. Notwithstanding the respective tensions, criminal activities committed through electronic channels due to the fact that the Information and Communication Technologies' (ICT) are developing are becoming "easier" and, therefore, the number of cybercrime cases and other criminal offences being executed based on telecommunication or public communication networks are increasing which is socially undesirable (Moore 2011, p. 4). Examples are data theft, identity theft, distribution of child pornography or copyright infringements.[26] For hampering the criminal prosecution a standard practice is to mask the used IP address (Graham, Howard and Olson 2011, p. 75). As a consequence, cyberspace, also referred to as the fifth common space,[27] "is in great need for coordination, cooperation and legal measures among all nations" (Schjølberg 2011, p. 2).

However, while some actions may be illegal in one part of the world, they may be legal in another area of the world since each State's national legislation differs from the one of other States. In this respect, the online world is similar to the offline world. Furthermore, with regard to the fact that access to the Internet can be achieved from almost every place on earth providing the necessary facilities, offenders very often operate from another part of the world (Moore 2011, p. 260). This aspect brings along further difficulties regarding the criminal prosecution: which States' relevant legislation will be applied in practice?

---

[25] ECHR, Appleby and Others vs. The United Kingdom, judgment of 6 May 2003, No. 44306/98, § 40.

[26] For more detailed information regarding the enforcement of copyright see Sect. 4.5.

[27] The four other spaces are land, sea, air and outer space.

Being a global problem, cybercrime must be understood from a global perspective. Effective cybercrime laws that are enforceable at national and international levels within a global and harmonized legal framework need to be developed, taking into account the Internet users' privacy. Insofar, public awareness of cybercrime and cybersecurity challenges will help to promote a cybersecurity culture.

Up to now, different efforts have been undertaken like the International Telecommunication Union's (ITU) Global Cybercrime Agenda, the subsequently founded ITU High-Level Expert Group, the Council of Europe's Convention on Cybercrime and several Framework Decisions and Directives of the European Union as set out hereinafter.

4.3.2 Global Cybersecurity Agenda

4.3.2.1 International Telecommunication Union

With governments realizing the growing importance of the new information and communication services, the International Telecommunication Union (ITU) passed a resolution in 1998 proposing the idea of a World Summit on the Information Society (WSIS) under the auspices of the United Nations. In 2001, the ITU Council endorsed the approach of holding the Summit in two phases, the first one in Geneva in 2003, the second one in Tunis two years later.

Being the United Nations specialized agency for information and communication technologies,[28] the ITU's activities focus on three main areas of activity, namely radio communication, standardization and development. In particular, the ITU coordinates the shared global use of the radio spectrum, promotes international cooperation in assigning satellite orbits, works to improve telecommunication infrastructure in the developing world and establishes worldwide standards.

Both World Summits on the Information Society highlighted security as a main pillar for building a stable global information society (Weber 2009, pp. 31–36). Hence, the ITU together with partners from governments, industry, international organisations and civil society launched the Global Cybersecurity Agenda (GCA) on 17 May 2007 (ITU 2007, p. 5), seeking to encourage collaboration amongst all relevant partners (HLEG 2008, p. 1). In so doing, serious crimes in cyberspace should be established under international law, regardless of whether they are chargeable under the respective national law (Schjølberg 2011, p. 2).

Following the idea of coordinating the international response to the growing challenges to cybersecurity and thereby aiming at proposing solutions to enhance confidence and security in the use of ICT (ITU 2007, p. 5), the GCA was built on

[28] See homepage of the ITU, overview.

five strategic pillars, namely legal aspects, technical measures, organisational structures, capacity building and international cooperation (ITU 2007, p. 13).

The GCA's central element is the establishment of a High-Level Experts Group (HLEG) aiming at refining the initial items listed on the Cybercrime Agenda (ITU 2007, p. 16); in particular the following objectives should be achieved: (1) the development of a model cybercrime legislation and a strategy to establish globally accepted minimum security criteria and accreditation schemes for software applications and systems taking into account existing public and private initiatives, (2) the creation and endorsement of a generic policy model and national strategies to develop appropriate national and regional structures to deal with cybercrime, (3) the establishment of a framework for watch, warning and incidents response, (4) the creation and endorsement of a universal generic identity framework to ensure the recognition of digital credentials for citizens across geographical boundaries, (5) the development of a global strategy to facilitate human and institutional capacity building and (6) the establishment of a global multi-stakeholder strategy to support and promote international cooperation for reaching all these goals mentioned above.

4.3.2.2 High-Level Experts Group

In order to fulfil the GCA's objectives the said High-Level Experts Group (HLEG) was established in 2007. Consisting of more than 100 experts from the fields of policy-making, academia, government and even the private sector (HLEG 2008, p. 2) the HLEG is subdivided into five working groups among others dealing with legislation, technological aspects, organisational aspects and the international cooperation among the Members.

To serve the Expert Group's main purpose of using "recognized sources of expertise in order to develop and propose practical solutions to facilitate the achievement of well-defined ITU strategic goals in cyberspace" (ITU 2007, p. 18), already in September 2008 the HLEG delivered a Chairman's Report (HLEG 2008, p. 191), comprising specific recommendations on cybercrime legislations by putting forward strategies regarding the aforementioned five work areas (ITU 2007, p. 16; HLEG 2008, p. 4). Additionally, the HLEG delivered a Global Strategic Report in November 2008,[29] including strategies in the five[30] work areas and summarizing the HLEG's work in seeking to promote cybersecurity around the world.

[29] HLEG Global Strategic Report 2008, http://www.itu.int/osg/csd/cybersecurity/gca/docs/global_strategic_report.pdf.

[30] The five work areas are legal measures, technical and procedural measures, organisational structures, capacity building and international cooperation, see supra note 30.

4.3.2.3 Implementation of the Global Cybersecurity Agenda

Since the GCA's launch in 2007, the composition has attracted the support and recognition of States and cybersecurity experts around the world and has promoted a number of initiatives, such as the ITU Child Online Protection Initiative that has been established in 2008 as an international collaborative network to promote the online protection of children worldwide by providing guidance on safe online behaviour.[31]

During the 2011 World Summit for Information Society Forum in Geneva, the ITU signed an agreement with the International Multilateral Partnership Against Cyber Threats (IMPACT), a not-for-profit comprehensive global public–private partnership alliance against cyber threats, making IMPACT the cybersecurity executing arm of the ITU as of September 9, 2011.[32] Being tasked with the responsibility of providing cybersecurity assistance and support to ITU's 193 Member States and also to other organisations within the UN system the ITU's GCA in collaboration with IMPACT is deploying security solutions to countries around the world.

4.3.3 Cybercrime Convention of Council of Europe

Since a harmonizing solution to combat cybercrime is needed, on the regional level already in 2001 the Council of Europe Convention on Cybercrime (Council of Europe 2004), the first international treaty seeking to address computer crime and Internet crimes by harmonizing national laws, appeared on the scene.

Having been developed between 1997 and 2000 by the Committee of Experts on Crime in Cyberspace (Gercke 2011, p. 142) the Convention on Cybercrime, also known as Budapest Convention on Cybercrime, was adopted by the Committee of Ministers of the Council of Europe on 8 November 2001 and entered into force on 1 July 2004. Later on, the Convention on Cybercrime was completed

[31] The ITU launched the Child Online Protection Initiative together with several UN agencies. The initiative's key objectives are among others the identification of risks to children in cyberspace, the creation of awareness and the development of practical tools for minimizing risks; see http://www.itu.int/osg/csd/cybersecurity/gca/cop/.

[32] The ITU considered the collaboration as "the world's first comprehensive alliance against cyberthreats"; see speech by ITU Secretary-General Dr Hamadoun I. Touréhttp, opening ceremony of the WSIS Forum, 16 May 2011, http://www.itu.int/en/osg/speeches/Pages/2011-05-16.aspx.

by the Additional Protocol to the Convention on cybercrime (Additional Protocol) (Council of Europe 2006),[33] entering into force on 1 March 2006.[34]

Seeking to "pursue, as a matter of priority, a common criminal policy aimed at the protection of society against cybercrime, inter alia, by adopting appropriate legislation and fostering international co-operation" (Council of Europe 2004: preamble), the Convention on Cybercrime aims at harmonizing the Member Countries' criminal regulations among others focussing on high-technology crimes such as illegal hacking into computer systems (Article 5), data piracy (Article 3), copyright infringements (Article 10), forgery and fraud (Article 7, 8), and the manufacture and distribution of child pornography (Article 9).

The Convention on Cybercrime serves as a guideline or as a reference for developing internal legislation by implementing its standards and principles in accordance with the local legal system and practice.[35] For standardizing the variety of national criminal regulations, to date, 47 States signed the Convention, even though just 32 States ratified the Convention. This numerical discrepancy among others refers to the fact that some of the Cybercrime Convention's criminalized actions are in conflict with the legal assessment of some Member States (Moore 2011, p. 261). By way of example, Article 5 of the Additional Protocol to the Convention on Cybercrime (Council of Europe 2006) is criminalizing hate speech; this legal provision might contradict the United States' First Amendment's guarantee of free speech[36]; similar legal problems occur related to the issue of child pornography (Moore 2011, p. 261).

Being based on criminal cyber-conducts in the late 1990s the Convention on Cybercrime does not cover new methods of conduct in cyberspace with criminal intent, such as phishing, botnets, spam, identity theft, crime in virtual worlds, terrorist use of the Internet, and massive and coordinated cyber-attacks against information infrastructures. In addition, the terminology included in the Convention turns out to be a 1990s terminology which is not necessarily suitable for the second decade of the 21st century. Hence, with regard to the use of anonymizing services[37] on the Internet the Convention on Cybercrime contains no specific regulations; the Convention "solely" introduces a regulatory framework for its Member Countries to handle criminal actions related to the World Wide Web.

---

[33] The Additional Protocol to the Convention on Cybercrime was adopted by the Council of Europe Committee of Ministers on 7 November 2002, open also to non-CoE-countries.

[34] States having ratified the Additional Protocol are requested to criminalize the dissemination of racist and xenophobic material and xenophobic-motivated threats and results through computer systems.

[35] Schjølberg and Ghernaouti-Hélie 2009 with a detailed proposal for a preliminary Model Law on Cybercrime Legislation based on the recommendations that were adopted in a broad agreement by the global High-Level Experts Group on Cybersecurity (for HLEG see 4.3.2.2), and recommendations on additional provisions due to the technological development since 2001.

[36] For more details regarding the U.S. Supreme Court's standpoint regarding the relationship between the First Amendment and defamation see Solove 2007, p. 125.

[37] See Sect. 2.2.

However, the Convention on Cybercrime also encompasses regulations allowing for a greater cooperation between law enforcement agencies and Internet Service Providers (ISPs) by determining the conditions in which ISPs are obliged to provide information (Moore 2011, p. 261) about their user to government agents (Article 18 para 1 lit. b Convention on Cybercrime). Due to the fact that anonymous acting on the Internet and the disclosure of information concerning a specific Internet user are inconsistent with one another, making reference to the Convention on Cybercrime is not that suitable to justify a right to act anonymously on the Internet.

4.3.4 EU Agenda

For the Council of Europe's (CoE's) non-Member Countries the Convention on Cybercrime serves as a central source to bring these countries' legislation towards European standards (Gercke 2011, p. 143). With regard to the CoE's Convention of Cybercrime's practical relevance for Member States of the EU, within the last ten years the EU has developed a number of legal frameworks for advancing the fight against cybercrime, among others the (1) Framework Decision on Combating Fraud (Council of the European Union 2001), (2) the Framework Decision on Attacks against Information Systems (Council of the European Union 2005), (3) the European Data Retention Directive (European Parliament 1995) and the (4) Amendment of the Framework Decision on Combating Terrorism (Council of the European Union 2008). Unlike the Council of Europe combining 47 Member States, all 27 Member States of the EU have to implement the aforementioned EU instruments within a given time frame (Gercke 2011, p. 143).

1. The Framework Decision on Combating Fraud of 2001 aims at assisting the European Union's fight against fraud and counterfeiting involving non-cash means of payment (Council of the European Union 2001: considerations 1, 5).[38] Therefore, the Framework Decision on Combating Fraud obligates all Member States to implement necessary measures to ensure the liability of legal persons intentionally committing one of the criminal offences listed in Article 2, as for instance theft or counterfeiting of a payment instrument in order for it to be used fraudulently.
2. Later on in 2005 the Framework Decision on Attacks against Information Systems was adopted, pursuing the goal to advance the cooperation between judicial and other competent authorities in the area of attacks against information systems (Council of the European Union 2005: consideration 1), by obliging all Member States "to take the necessary measures to ensure that the

[38] Fraud and counterfeiting of non-cash means of payment often operate on an international scale.

intentional access without right to the whole ore any part of an information system is punishable as a criminal offence" (Article 2) within the given transition period.
3. Subsequently, the European Parliament and the Council of the European Union adopted the Data Retention Directive, as set out above, aiming at harmonising all Member States' regulations for establishing a framework to enable law enforcement authorities and intelligence agencies to access stored communications, traffic and location data, thereby improving criminal investigations.
4. Furthermore, the Amendment of the Framework Decision on Combating Terrorism needs to be mentioned, updating the Council Framework Decision of 13 June 2002 on Combating Terrorism. Including new offences, namely public provocation to commit a terrorist offence, recruitment and training for terrorism, also when committed through the World Wide Web, the Amendment and the underlying Framework Decision constitute a key tool in the fight against terrorism and aim at harmonizing respective national provisions.

Similarly to the Convention on Cybercrime, the EU Framework Decision on Combating Fraud, the Framework Decision on Attacks against Information Systems, the Data Retention Directive and the Amendment of the Framework Decision on Combating Terrorism do not contain specific conditions to substantiate a right to act anonymously on the Internet (by using anonymizers). In fact, a justification of such a right would adversely affect the Framework Decisions' and Directive's fundamental idea of improving prosecution in the case of criminal actions committed on the Internet.

4.4 Supervising Internet Traffic by Trojan Horse Software

4.4.1 Use of Trojan Horse Software by the German Government

In the context of conflicting interests between the Internet participants' privacy and the States' duty to protect governments partially draw on illegal measures, as shown by the German Chaos Computer Club (CCC)[39] in respect of the recently

[39] Claiming to be the "largest European hacker club" (CCC 2011a), the German hacker association CCC founded in Berlin, Germany, in 1981 and based in Germany and other German-speaking countries assesses itself as a mediator between the poles of technical and social development. According to its preamble, the CCC urges for the appreciation of the right to a worldwide, unhampered information exchange as being a human right since within today's information society living and working without Internet access is almost inconceivable (CCC 2011b). Furthermore, the CCC stands up for more transparency in governments, freedom of information and fights for everyman's right for free universal access to computers and technological infrastructure. The political activities of the Chaos Computer Club bear on the revelation of shortcomings and the disclosure of security loopholes, partially by intentionally breaking through existing safety appliances as undertaken in 1996 by demonstrating an attack against Microsoft's ActiveX technology.

revealed potentially unconstitutional use of Trojan horse software by German investigators. In addition to this occurrence also other governments made use of the Trojan horse software.

4.4.1.1 Trojan Horse Software

(1) Trojan Horse Mythology

According to the Greek mythology, within the Trojan War the Greeks finally entered the city of Troy and ended the conflict by outflanking the Trojans. The Greeks constructed a huge wooden horse, presented it to the Trojans and made the Trojans belief that they sailed away. Thereupon, the Trojans opened their gates and pulled the horse into their city unknowingly that they let the enemy in since the Greeks had hidden a select force of men inside the horse. In the course of the following night the Greeks came out of the horse, opened the gates for the rest of their secretly resailed army and overwhelmed the sleeping Trojans.

(2) Trojan Horse Software

Referring to the aforementioned incident of Greek warriors sneaking inside the city of Troy (Moore 2011, p. 38), "Trojan Horse Software" (also referred to as Trojans)[40] means a computer program not knowingly installed by the computer's user that appears at a first glance as a useful program but performs a different task unknown to the person concerned (Graham Howard and Olson 2011, p. 92).[41]

The Trojan himself is not a computer virus and is not necessarily harmful. However, this software is often combined with further malicious software or enables malicious software to get onto the computer unnoticed, as for example so-called keyloggers that records keyboard or mouse movements and thus collect unencrypted data and passwords. Therefore, Trojans belong to the so-called malware, the unsolicited and harmful programs.[42]

The Trojan Horse Software's installation happens by the safety authority through physical access to the communication device or by the users themselves, either undetected via an email attachment (Moore 2011, p. 38)[43] or as a result of fraudulent representations in terms of the respective purpose of use (Braun and Roggenkamp 2011, p. 681). In both cases applications are installed on the

[40] Even though this description is misleading since the Greeks finessed the Trojans and not vice versa.

[41] As for instance applications that pretend to be antivirus programs.

[42] See R. Moir, Defining Malware: FAQ, 1 October 2003, http://technet.microsoft.com/en-us/library/dd632948.aspx.

[43] Trojan horses are often sent to a computers via email to legitimate users of the system.

communication devices of the persons concerned without their knowledge and their consent. The Trojans among others may be programmed to activate when an executive instruction is given to start a particular computer program or when the recipient of the contaminated email unwittingly activates the file (Moore 2011, p. 38).

The installation and activation of the malware enables the hacker to have access to the computer remotely and perform various operations like eavesdropping the complete Internet communication, down- or uploading of files, installation of software/further malware on the "captured" computer, or committing data theft by emailing password lists to the owner of the Trojan program (Moore 2011, p. 38). Insofar, Trojans have all the attributes to accomplish both a lawful interception[44] and the more extensive online surveillance.[45]

4.4.1.2 The German "Bundestrojaner"

(1) Disclosure by the Chaos Computer Club

According to the Chaos Computer Club, the software, reportedly developed by a Hessian company,[46] was among others used by Bavarian law-enforcement[47] officials and was played into the hackers' hands without being asked (CCC 2011c, p. 1). Having examined the transmitted German governmental software in detail, the Chaos Computer Club on 8 October 2011 disclosed the use of a "lawful interception malware program by German police forces" (CCC 2011a), since then better known as the Bundestrojaner or Staatstrojaner, a Federal Trojan horse software.[48]

---

[44] The often used term lawful interception, also referred to as wiretapping, directly at the source ("source wiretapping") (CCC 2011a) of the communication, describes the monitoring of a suspect's Internet telephony by accessing to one of the end-devices involved using Trojan horse software. By definition, this procedure can only be used for wiretapping Internet telephony; the solely usage for conducting a lawful interception has to be enforced by appropriate technical and legal means (CCC 2011a). Moreover, for the protection of the overheard person's human rights, the conduct of a lawful interception requires a warrant; the Global Lawful Interception Industry Forum lists many of these different legislations, as does the Council of Europe secretariat. For example, in the United Kingdom the law is known as RIPA (Regulation of Investigatory Powers Act) and in the United States there is an array of federal and state criminal law, in particular the Communications Assistance for Law Enforcement Act (CALEA).

[45] See supra note 36.

[46] The investigated Trojan was developed by the company DigiTask; see exemplary Rosenbach, Stark and Winter 2011.

[47] The software in question was used by various state officials, see exemplary Rosenbach Stark and Winter 2011; German news agency 2011.

[48] The term "Bundestrojaner" is colloquially used to describe the government malware concept (CCC 2011a). The software is also referred to as R2D2, see exemplary: http://cetatti.com/blog/2011/10/german-officials-admit-to-using-r2d2-trojan-to-spy-on-citizens/.

Primarily, the computer surveillance program "Bundestrojaner" was developed to monitor suspects' Internet telephone calls via providers like Skype, a software application allowing its users to make partially free[49] telephone calls (voice and video) over the Internet. Since Internet telephony programs usually encrypt the data before they leave the sender's computer, the monitoring of the suspect's computer requires the controller's access to one of the end-devices involved (Braun and Roggenkamp 2011, p. 681).

Officially, the Trojan horse software was designed for the use on Windows operating systems for the recording of Voice over Internet Protocol (VoIP) telephone calls and for making screenshots of the reviewed computers, i.e. for accomplishing lawful interceptions of suspects.[50]

After having been passed the software in question, the CCC published the extracted binary files of the applied software used by the German investigators on their website (CCC 2011a), complemented by a report about the range of functions and an evaluation of the technical analysis (Braun and Roggenkamp 2011, p. 681). Subsequently, the CCC received a newer version (CCC 2011d) of the government spyware, publishing her findings on October 26, 2011 (CCC 2011e).

The first version of the Bundestrojaner passed to the Chaos Computer Club was assigned for wiretapping suspects' Internet telephone calls and for making screenshots of the reviewed computers (CCC 2011c, p. 2). As appears from the CCC's reports, the developed malware contains further functions which can easily be activated afterwards and enables the respective operator to install and run software on the tapped computer, monitor the online activity of the infected computer, scan and even manipulate the data stored on the computer and update its functionality via the Internet (CCC 2011c, p. 2).[51] Even though the later passed federal Trojan's basic version does no longer contain the possibility to copy the screenshot of the suspect's computer, the malware's range of application can be extended easily (CCC 2011f).

Hence, the said software has all the attributes to accomplish an online surveillance; beyond that even electronic eavesdropping operation (room surveillance) is possible by activating the computer's hardware (camera and/or microphone) from a distance (CCC 2011a). Since the Trojan's design and implementations involves the risk of "making all the functionality available to anyone on the Internet", the device uncloses a security loophole on the suspect's computer (CCC 2011a).

According to the CCC, this additional application's spectrum (over and above lawful interception) was "hidden" within the software on purpose as to enable the

[49] Telephone calls made by using the software application "Skype" to a recipient simultaneously using the application "Skype" are free of charge. Additionally, "Skype" enables its users to do instant messaging, to transfer files and to do videoconferencing over the Internet.

[50] See supra note 45.

[51] Beyond that the Bundestrojaner is said to be capable of monitoring traffic from 15 programs, see Constantin 2011.

enlargement of the suspects' spy out on demand beyond the allowed without additional judicial writ (CCC 2011c, p. 11, 15).

The server's IP address linking to a computer belonging to an US American computer center was firmly fixed "within" the Trojan software.[52] As a result, all tracked data were delivered to the United States first before they reached the respective German authorities (Tschentscher 2011, p. 21). Even though all data transmitted have been encoded, security gaps cannot be avoided since the same code was deployed within all examined versions of the software (Braun and Roggenkamp 2011, p. 682). Furthermore, a codification of inbound commands and a control of whether all these commands really originated from the US American server did not take place making the network's fraudulent manipulation technically possible.[53] Reportedly, installations of spyware utilized by German investigators were accomplished at the terminal device, some of them secretly during a customs control (Rosenbach et al. 2011; Braun and Roggenkamp 2011, p. 681).

In the course of the Trojan's disclosure by the CCC the issue was debated which technologies German law-enforcement officials are allowed to apply while investigating suspected criminals (Rosenbach et al. 2011) and if so whether the usage is undermining the ruling set in place by the February 27, 2008 German Federal Constitutional Court Ruling on the subject of online surveillance (German Federal Constitutional Court 2008), among others ruling the secret infiltration of information technology systems of being an infringement of the general personality right.[54]

(2) Legal Consequences of Malware Utilization

Due to the fact that there is no respective statutory rule existing in the German Code of Criminal Procedure,[55] the accomplishment of online surveillances for criminal prosecution is de lege lata illegitimate (Braun and Roggenkamp 2011, p. 682). According to the German Constitutional Court the accomplishment of source wiretapping also poses a threat to the basic law on IT, since the required infiltration of a computer effectively removes the crucial hurdle to spy out the information technology system at all (German Federal Constitutional Court 2008: Sect. 204).

Accordingly, the accomplishment of a lawful interception also requires a specific parent act (Braun and Roggenkamp 2011, p. 683 with further references). In this respect, the opinions are divided as to whether a source wiretapping can be based on the parent act of an "ordinary" telephone surveillance. While court

[52] The command and control server is located on an IP address belonging to the provider Web intellects in Columbus, Ohio; (CCC 2011c, p. 3).

[53] Hence, the networks remote control and tempering by third parties cannot be precluded; (CCC 2011c, p. 4).

[54] See Sect. 4.2.2.

[55] The German Code of Criminal Procedure (StPO).

practice and the legal doctrine partly base source wiretapping on Articles 100 a, b German Code of Criminal Procedure, the fact that telephone surveillances does not require access to the target subject's computer inter alia contradicts the equal treatment (Braun and Roggenkamp 2011, p. 683 with further references).

The Bundestrojaner's[56] legitimacy requires the existence of both software in conformity with the law and a provision authorizing the measure which is in accordance with the Constitutional Court Ruling (Braun and Roggenkamp 2011, p. 686).

Supposed, the legitimacy of using Trojans in general can be based on the German Code of Criminal Procedure, the application of the respective versions investigated by the CCC might have been unlawful (Braun and Roggenkamp 2011, p. 684). Basic principles of data protection law have been neglected since the tracked data passed unsecured networks (CCC 2011c, p. 6). Furthermore, with regard to the aforementioned missing parent act, the Trojan's implementation for accomplishing online surveillances was illegitimate.

Fuelled by the CCC's decryption of the Bundestrojaner the debate about Internet monitoring including the discussion about the right to remain and act anonymous on the Internet reaches a new intensity (Tschentscher 2011, p. 279). In consideration of the public debate about the existence and risk of terrorist structures within the right-wing scene[57] and the concomitant repeated calls for a party ban of the NPD[58] the Court Ruling on online surveillance could become subject to reconsideration in the future.

4.4.2 Use of Trojan Horse Software by Other Governments

4.4.2.1 Switzerland

Besides Germany also Switzerland[59] admitted the purchase and using of a particular type of computer spy software currently stirring debate in Germany (Weber et al. 2012, p. 6).[60]

Following the detection of the repeated use of Federal Trojans by German authorities and the subsequent concession of Swiss criminal prosecution authorities of having applied similar measures for conducting Internet surveillances, the Swiss Federal Council aims at precisely regulating the dealing with monitoring software. Since there is to date some disagreement about the existence of a legal

---

[56] For accomplishing lawful interceptions and online surveillances.

[57] In November 2011, German authorities discovered a neo-Nazi terror cell in Germany.

[58] The National Democratic Party of Germany is a far-right political party in Germany.

[59] Miscellaneous contributions in Swiss newspapers, see exemplary Schaffner 2011, p. 4 or Fontana 2011, p. 12.

[60] See Tschentscher 2011 and miscellaneous online contributions exemplary: http://www.eurasiareview.com/15102011-switzerland-law-enforcement-admits-use-of-spy-software/ and http://worldradio.ch/wrs/news/wrsnews/switzerland-admits-using-spy-software~print.shtml.

basis, the Swiss Federal Council plans to submit a draft proposal for the revision (Swiss Federal Data Protection Commissioner 2010/2011) of the Federal Law on the Surveillance of Postal and Telecommunications Traffic (Federal Assembly of the Swiss Confederation 2000), thereby creating more legal stability in dealing with Federal Trojans.

To date, Switzerland does not know a comparable right to the German right to confidentiality and integrity of information technology systems (Tschentscher 2011; Weber 2008). Instead, the surveillance of private computers with the aid of Trojans can affect a variety of fundamental rights, like for instance data protection, privacy, confidentiality of communication and personal liberty (Federal Constitution of the Swiss Confederation 1999; Tschentscher 2011). In contrast to the legal situation in Germany, the Swiss Federal Constitution in Article 13 codifies the right to privacy, awarding "everyone […] the right to privacy in their private and family life and in their home, and in relation to their mail and telecommunications" and that "the right to be protected against the misuse of their personal data" (Federal Constitution of the Swiss Confederation 1999).

Aiming at bringing the Federal Law on the Surveillance of Postal and Telecommunications Traffic (Federal Assembly of the Swiss Confederation 2000) into line with the recent technological developments, the Federal Council's draft proposal explicitly includes the Internet, namely Internet telephony and emails (Swiss Federal Data Protection Commissioner 2010/2011). The draft proposal (Swiss Federal Data Protection Commissioner 2010/2011), in principle, authorizes Swiss governmental authorities to use monitoring software, although with narrow limits, to avoid the systematic monitoring in advance. Therefore, the draft proposal intends to set more restrictive conditions for the surveillance of a suspect's computer using Trojans compared to the regular telephone and Internet surveillance. In addition to the previous order by a public prosecutor and a judicial approval the employment of Trojans requires as further condition the prosecution of offences meeting the qualifications for an undercover investigation (Fontana 2011).

Beyond that, the draft reduces the surveillance to encrypted transmitted data like mails or communication via Skype; the recording of passwords, searching of hard discs or room monitoring by accessing a computer's microphone and camera are not included (Fontana 2011; Schaffner 2011). Since the draft proposal is expected to come into force only within the next two or three years, the legal situation currently remains unclear.

In addition to the pending revision of the Federal Law on the Surveillance of Postal and Telecommunications Traffic the Swiss Federal Council announced amendments[61] to the Regulation on the Surveillance of Postal and Telecommunications Traffic (Swiss Federal Council 2001) to clarify which Internet Service Providers would obliged to deliver data to Swiss law enforcement authorities.

[61] The Swiss Federal Council implemented the revised Regulation on the Surveillance of Post and Telecommunications Traffic starting January 1, 2012, see http://www.admin.ch/aktuell/00089/index.html?lang=de&msg-id=42332.

According to the revised Regulation the Internet Access Providers are obliged to deliver data to Swiss law enforcement authorities; providers of chats or blogs only and providers of private networks are exempted from this duty (Swiss Federal Data Protection Commissioner 2010/2011).

4.4.2.2 Austria

Reportedly, the program has also been sold to State agencies in Austria (Bobi 2011). According to Digitask, the developer of the Bundestrojaner,[62] Austrian government authorities at least once acquired a highly controversial computer program, in that the case the so-called "Remote Forensic Software" (Bobi 2011; Austrian Federal Ministry of Justice 2008, p. 15).

Current findings point to the fact that Austrian authorities illegally used the control and monitoring software. The monitoring of message-related computer applications like Email or Voice over Internet Protocols (VoIP) can take place in conformity with the law but enabling the software's user to enter the targeted computer by use of Trojans to investigate the computer from the outside, therewith accomplishing an online surveillance, cannot be based on a parent act within Austria (Austrian Federal Ministry of Justice 2008, p. 33).

4.4.3 Concluding Legal Assessment

Even though each individual country has different legal requirements relating to the lawfulness of interceptions[63] and online surveillance,[64] the above described Council of Europe's Convention on Cybercrime[65] can be seen as a guideline for developing internal legislation; in this legal instrument, Article 19 is relevant regarding online surveillance and Articles 20 and 21 deal with interception.

Article 19 of the Convention (Council of Europe 2004)[66] states, that each signatory State "shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access a computer system or part of it and computer data stored therein; and a computer-data storage medium in which computer data may be stored in its territory".

Article 20 of the Convention addresses the real-time collection of traffic data. According to Article 21 of the Convention, addressing the interception of content data, among others "each Party shall adopt such legislative and other measures as

[62] See Sect. 4.4.1.2.

[63] See supra note 45.

[64] Commonly a warrant is needed to accomplish a lawful interception or online search.

[65] See Sect. 4.3.3.

[66] Article 19: Search and seizure of stored computer data.

may be necessary, in relation to a range of serious offences to be determined by domestic law, to empower its competent authorities to collect or record through the application of technical means on the territory of that Party and compel a service provider, within its existing technical capability to collect or record through the application of technical means on the territory of that Party, or to co-operate and assist the competent authorities in the collection or recording of, content data, in real-time, of specified communications in its territory transmitted by means of a computer system […]".

Giving online surveillance and interceptions a solid legal basis is expected to contribute to the freedom and fundamental rights of each individual citizen. Adopting legislative measures to empower the competent authorities contributes to stable jurisprudence and to provide legal certainty. To date several countries which have signed the Convention still lack of any explicit reference; accordingly there are still efforts needed to satisfactory fulfill the Convention on Cybercrime.

4.5 Enforcement of Copyright

In parallel to the augmented use of the globally available World Wide Web as communication tool, illegal activities and/or preliminary measures thereto increasingly shift from the real into the online world and concomitant among others a new field of activity for copyright infringements appeared on the scene, namely within file-sharing sites and on Internet marketplaces like eBay. Internet users among others download music illegally by simultaneously putting them on the market or use copyright reserved picture files within the frame of (private or commercial) Internet auctions. Supported by the existing and above described opportunities to act anonymously on the Internet[67] copyright infringers to a great extent get away without punishment.[68]

Within the last years repeatedly (beginning with the famous Napster case at the beginning of this century) corresponding Internet portals emerged (and for the most part disappeared a little while later), like the recently blocked online storage and file delivery service "Megaupload.com" or the German website "kino.to".

"Kino.to" was a German-speaking video on demand website for cinematographic works, television series and TV reports best-known for copying and viewing pirated audiovisual content.[69] Held and controlled by anonymous users the website's access was blocked due to violations of copyright law in June 2011.

---

[67] See Sect. 2.2.

[68] In recent years a number of attorneys specialized on copyright law whereby the dispatch of cease-and-desist letters increased.

[69] The purpose of "Kino.to" was to collect links to attractive audiovisual content and to promote these links at the website next to advertisements. These advertisements to a great extent contained illegal material themselves, such as links to destructive software or deceptive web services; for further details see Moeller 2011.

Up to its shut down by German authorities the website was told to be one of the 50 most popular German websites.

In the case of the storage service "Megaupload.com" on January 19, 2012, US Federal authorities shut down one of the Internet's most popular websites as part of an indictment accusing the operators of the website of running an international criminal organisation allowing Internet participants to easily watch or share pirated content of numerous types of copyrighted works (Horwitz and Kang 2012). According to a statement of the US Justice Department "this action is among the largest criminal copyright cases ever brought by the United States" since "the estimated harm caused by the conspiracy's criminal conduct to copyright holder is well in excess of $500 million" (US Department of Justice 2012).

Immediately after the website's shutdown and the arrest of seven executives including the company's founder,[70] the activists of "Anonymous"[71] announced revenge in the form of an "operation payback"[72] and threatened to take several popular websites offline, among others of the Federal Bureau of Investigation (FBI), the US Department of Justice and the Motion Pictures Association of America (Horwitz and Kang 2012). Shortly afterwards, "Anonymous" carried out their threats by temporarily shutting down ten websites, among them the US Department of Justice's website, with a distributed denial of service attack (DDoS)[73] (Ralph 2012). For this purpose, a large number of activists using Low Orbit Ion Cannon (LOIC)[74] simultaneously sent network traffic like senseless Internet inquiries to the targeted website(s) and therewith (in that event) overloaded the Department of Justice's website.

Related to the augmented emergence of file-sharing sites etc. and the therein committed copyright infringements a new field of activity for lawyers emerged and, accordingly, in recent years a number of attorneys specialized on copyright law. Even though in the course of the increasing dispatch of cease-and-desist letters the awareness of Internet copyright infringements has increased a little, many Internet participants still held copyright infringements of being only trivial offences.

With regard to these conflicting opinions it is still to be clarified whose "right" prevails, the privacy of the respective file-sharer trying to hide his identity by acting anonymously within the World Wide Web or the right holders' copyright and consequently their demand for gathering information from the Internet Service Providers about violators by disclosure of the used IP addresses for enforcing their rights.

---

[70] "Megaupload.com" is led by Kim Dotcom, formerly known as Kim Schmitz or Kim Tim Jim Vestor, a German entrepreneur living in Auckland, New Zealand, and having his place in business in Hong Kong.

[71] See supra note 20.

[72] Anonymous' "operation payback" describes a decentralized and coordinated group of attacks on opponents of Internet piracy and pro-copyright organisations starting in 2010.

[73] See Sect. 2.1.3.

[74] LOIC is an open source network stress testing and denial-of-service attack application.

According to the latest jurisdiction of the Court of Appeal of the Swiss canton Berne, IP addresses collected by a private firm using discovery software are to be considered as illegally "acquired" (Weber 2011c, pp. 28/29) and may not be used for Internet participants' identification (Berne Court of Appeal 2011). In this particular case,[75] a holder of rights in music titles filed a criminal complaint with the prosecution authorities on the basis of 531 IP addresses collected by a private firm, potentially belonging to persons having illegally downloaded music titles. The copyright holder asked the authorities to request from the relevant Internet Service Providers disclosure of the Internet users' real names and addresses belonging to these IP addresses. The authorities imposed a cost advance on the complainant arguing that the request would mainly serve the enforcement of civil law rights.

The Court held that the complainant would mainly be interested in gathering evidence for the enforcement of civil law rights based on an alleged violation of Copyright Law through the criminal prosecution. Irrespective of the question whether such procedural step would be justified the Court of Appeal expressed the opinion that at first instance the legality of collecting the 531 IP addresses by a private firm had to be assessed. Thereby, the Court of Appeal relied on the *Logistep* decision[76] of the Swiss Federal Court of 8 September 2010 indicating that Copyright Law may not enjoy a higher value than Data Protection Law (Swiss Federal Court 2010).[77] According to the Swiss Federal Court, private (economic) interests in having others complying with Copyright Law cannot outweigh the interest of an individual in having his/her data protected from being disclosed; data protection includes an element of public interest and, therefore, prevails under the given circumstances. Consequently, information gained and collected by a private firm in relation to IP addresses without the consent of the concerned individual is to be considered as illegally "required" information and may not be used as evidence in proceedings, unless a specific exemption applies.

Summarizing, on the one side Internet users participating in peer-to-peer-networks[78] sites argue that their IP addresses are tantamount to personal data and therewith are in need of protection since Copyright Law may not enjoy a higher value than Data Protection Law (Weber 2011b, pp. 191/192). Right holders on the other side fear for the violation of their rights by simultaneously feeling incapable to protect their "property" and due to that seek for the divulgence of the used IP addresses, if necessary with the aid of specialized business models.

---

[75] The subsequent passage is partly based on Weber 2011c.

[76] The business model of Logistep AG, a Swiss enterprise, consists in collecting IP addresses of Internet users who participate in P2P networks and make available works, protected by Copyright Law, to third persons without having the copyright holder's permission. Acting (at least indirectly) on behalf of the right holders Logistep delivers the respective IP addresses to the prosecutors in criminal proceedings enabling them to request from the relevant Internet Service Providers the disclosure of the name of the respective Internet participant; for more detailed information see Weber 2011b.

[77] In that case both static and dynamic IP addresses were qualified as personal data.

[78] See Sect. 2.2.2.

Regarding this issue, Article 10 para 1 of the Convention of Cybercrime[79] might be of interest, stating that "each party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of copyright […] where such acts are committed willfully, on a commercial scale and by means of a computer system" (Council of Europe 2004). Since this Convention's provision makes commercial scale a condition and a substantial percentage of Internet participants committing copyright infringements (by among others using file-sharing sites etc.) are private persons the Convention of Cybercrime does not concern these infringements.

References

Austrian Federal Ministry of Justice (2008) Final report of the Austrian working group on online surveillance. 9 April 2008. http://www.webinformation.at/material/AG_OnlineDurchsuchung_Endbericht.pdf. Accessed 31 Jan 2012

Barlow JP (1996) A declaration of the independence of cyberspace. 9 February 1996. http://w2.eff.org/Censorship/Internet_censorship_bills/barlow_0296.declaration. Accessed 31 Jan 2012

Berne Court of Appeal (2011) Decision of 22 March 2011. Canton of Berne. http://www.grundrechte.ch/2011/og_bk_11_9. Accessed 31 Jan 2012

Bobi E (2011) Trojanische Sitten: Der Bundestrojaner wurde ohne rechtliche Grundlage eingesetzt. profil online. 22 October 2011. http://www.profil.at/articles/1142/560/310153/bundestrojaner-trojanische-sitten. Accessed 31 Jan 2012

Braun F, Roggenkamp JD (2011) 0zapftis—(Un)Zulässigkeit von "Staatstrojanern". Kommunikation Recht 11:681–686

Chaos Computer Club (2011) Chaos computer club analyzes government malware. 8 October 2011. http://ccc.de/en/updates/2011/staatstrojaner. Accessed 31 Jan 2012.(CCC 2011a)

Chaos Computer Club (2011) Bylaw. http://www.ccc.de/en/satzung. Accessed 31 Jan 2012. (CCC 2011b)

Chaos Computer Club (2011) Analyse einer Regierungs-Malware. 8 October 2011. http://www.ccc.de/system/uploads/76/original/staatstrojaner-report23.pdf. Accessed 31 Jan 2012. (CCC 2011c)

Chaos Computer Club (2011) Chaos computer club analyzes new German government spyware. 26 October 2011. http://www.ccc.de/en/updates/2011/analysiert-aktueller-staatstrojaner. Accessed 31 Jan 2012. (2011d)

Chaos Computer Club (2011) 0zapftis—Teil 2, Analyse einer Regierungs-Malware: Drei Jahre sind in der IT eine wirklich lange Zeit. 26 October 2011. http://www.ccc.de/system/uploads/83/original/staatstrojaner-report42.pdf. Accessed 31 Jan 2012. (CCC 2011e)

Chaos Computer Club (2011) Chaos computer club analysiert aktuelle Version des Staatstrojaners. 26 October 2011. http://www.ccc.de/de/updates/2011/analysiert-aktueller-staatstrojaner. Accessed 31 Jan 2012. (CCC 2011f)

Cottier T, Delimatsis P, Diebold NF (2008) Article XIV GATS. In: Wolfrum R, Stoll PT, Feinäugle C (eds) WTO—Trade in services. Martinus Nijhoff Publishers, Leiden and Boston

Council of Europe (1950) European convention for the protection of human rights and fundamental freedoms. 4 November 1950. http://conventions.coe.int/treaty/Commun/QueVoulezVous.asp?NT=005&CL=ENG. Accessed 31 Jan 2012

[79] See Sect. 4.3.3.

Council of Europe (2004) Convention on cybercrime. 23 Nov 2001. http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CM=8&DF=02/06/2010&CL=ENG. Accessed 31 Jan 2012

Council of Europe (2006) The additional protocol to the convention on cybercrime, concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems. http://conventions.coe.int/treaty/Commun/QueVoulezVous.asp?NT=189&CL=ENG. Accessed 31 Jan 2012

Council of the European Union (2001) Council framework decision of 28 May 2001 combating fraud and counterfeiting of non-cash means of payment. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2001:149:0001:0004:EN:PDF. Accessed 31 Jan 2012

Council of the European Union (2005) Council framework decision 2005/222/JHA of 24 February 2005 on attacks against information systems. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2005:069:0067:0071:EN:PDF. Accessed 31 Jan 2012

Council of the European Union (2008) Amendment of the framework decision on combating terrorism. 18 April 2008. http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/08/255. Accessed 31 Jan 2012

European Parliament (1995) Directive 95/46/EC of the European parliament and of the council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on free movement of such data. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:1995:281:0031:0050:EN:PDF. Accessed 31 Jan 2012

Federal Assembly of the Swiss Confederation (2000) Federal Law on the surveillance of post and telecommunications traffic. SR780.1. http://www.admin.ch/ch/d/sr/780_1/index.html. Accessed 31 Jan 2012

Federal Constitution of the Swiss Confederation (1999) SR 101. http://www.admin.ch/ch/e/rs/101/index.html. Accessed 31 Jan 2012

Fontana K (2011) Enge Grenzen für "Trojaner". Neue Zürcher Zeitung. No. 275. 24 Nov 2011: 12

Gercke M (2011) 10 years convention on cybercrime: achievements and failures of the council of europe's instrument in the fight against internet-related crimes. Comput Law Rev Int 5:142–149

German Federal Constitutional Court (2008) 1 BvR 370/07, 1 BvR 595/07. 27 February 2008. http://www.bverfg.de/entscheidungen/rs20080227_1bvr037007.html. Accessed 31 Jan 2012

Graham J, Howard R, Olson R (eds) (2011) Cyber security essentials. Auerbach Publications, Boca Raton

High-Level Experts Group (HLEG) (2008) Report of the chairman of HLEG. 3 September 2008. http://www.itu.int/osg/csd/cybersecurity/gca/docs/Report_of_the_Chairman_of_HLEG_to_ITU_SG_03_sept_08.pdf. Accessed 31 Jan 2012

Horwitz S, Kang C (2012) Federal indictment claims popular Web site Megaupload.com shared pirated material. The Washington Post. 20 January 2012. http://www.washingtonpost.com/business/economy/federal-indictment-claims-popular-web-site-shared-pirated-material/2012/01/19/gIQA4rDwBQ_print.html. Accessed 31 Jan 2012

International Telecommunication Union (ITU) (2007) Global cybersecurity agenda: framework for international cooperation in cybersecurity. http://www.ifap.ru/library/book169.pdf. Accessed 31 Jan 2012

Jackson M (2011) Right to privacy, unlawful search and surveillance. In: Chan J, Lim CL (eds) Law of the Hong Kong constitution. Sweet and Maxwell, Hong Kong

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

Munin N (2010) Legal guide to GATS. Kluwer Law International, The Netherlands

Ralph T (2012) Hacker collective anonymous shuts down department of justice website, among others. GlobalPost. 19 January 2012. http://www.globalpost.com/dispatch/news/business-tech/technology-news/120119/anonymous-hacks-DOJ-universal-websites-megaupload. Accessed 31 Jan 2012

Rosenbach M, Stark H, Winter S (2011) The shady past of Germany's Spyware. Spiegel online international. 17 October 2011. http://www.spiegel.de/international/germany/0,1518,792276,00.html. Accessed 31 Jan 2012

Ryga BM (1995) Cyberporn: Contemplating the first amendment in cyberspace. Seton Hall Const Law J 6:221–223

Schaffner D (2011) Sommaruga setzt der Überwachung im Internet nun Grenzen. Tagesanzeiger. 24 Nov 2011: 4

Schefer M (2001) Die Kerngehalte von Grundrechten: Geltung, Dogmatik, inhaltliche Ausgestaltung. Stämpfli, Berne

Schjølberg S, Ghernaouti-Hélie S (2011) Potential new global legal mechanisms on combating cybercrime and global cyberattacks. A presentation at the ISPAC International Conference on Cybercrime: Global Phenomenon and its Challenges. 2–4 December 2011. http://cybercrimelaw.net/documents/ISPAC.pdf. Accessed 31 Jan 2012

Solove DJ (2007) The Future of Reputation: Gossip, Rumor, and Privacy on the Internet. Yale University Press, New Haven

Swiss Federal Council (2001) Regulation on the surveillance of post and telecommunications traffic. SR.780.11. http://www.admin.ch/ch/d/sr/780_11/index.html. Accessed 31 Jan 2012

Swiss Federal Court (2010) Decision of 8 September 2010. http://jumpcgi.bger.ch/cgi-bin/JumpCGI?id=08.09.2010_1C_285/2009. Accessed 31 Jan 2012

Swiss Federal Data Protection Commissioner (2010/2011) Progress report 18: revision of the federal law on the surveillance of post and telecommunications traffic. http://www.edoeb.admin.ch/dokumentation/00445/00509/01732/01753/index.html?lang=de. Accessed 31 Jan 2012

Tschentscher A (2011) Computer-Grundrecht gegen "Staatstrojaner". Neue Zürcher Zeitung. 9 Nov 2011: 21

United Nations (1966) International covenant on civil and political rights. 16 December 1966. http://www2.ohchr.org/english/law/ccpr.htm. Accessed 31 Jan 2012

United States Department of Justice (2012) Justice department charges leaders of megaupload with widespread online copyright infringement. Office of Public Affairs. 19 January 2012. http://www.justice.gov/opa/pr/2012/January/12-crm-074.html. Accessed 31 Jan 2012

Weber RH, Sommerhalder M (2007) Das Recht der personenbezogenen Information. Schulthess/Nomos, Zurich

Weber RH (2008) Grundrecht auf Vertraulichkeit und Integrität. Digma 2:94–97

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

Weber RH (2011a) The right to be forgotten: more than a Pandora's Box? J Intellect Property Inf Technol E-Commer Law 2:120–130 (Weber 2011a)

Weber RH (2011b) Switzerland: private use of discovery software for IP addresses. Comput Law Rev Int 6:191–192 (Weber 2011b)

Weber RH (2011c) Legality of IP-address discovery software—Logistep. Comput Law Rev Int 1:28–29 (Weber 2011c)

Weber RH, Wolf CA, Heinrich UI (2012) Neue Brennpunkte im Verhältnis von Informationstechnologien, Datensammlungen und flexibilisierter Rechtsordnung. Jusletter. 12 March 2012. http://jusletter.weblaw.ch/article/de/_10019. Accessed 11 April 2012

Wildhaber L, Breitenmoser S (1992) Art. 8 EMRK. In: Golsong H, Karl W (eds) Internationaler Kommentar zur Europäischen Menschenrechtskommission. Commentary. Carl Heymanns Verlag, Cologne