Switzerland

Thomas Widmer and Deborah Lechtman,
LALIVE SA
Geneva, Switzerland

Introduction

In General

Switzerland's approach to the legal challenges raised by the Internet and other new information technologies has been one of ongoing cautious adjustments.[1] Legislative steps have been taken primarily in response to legal developments taking place elsewhere, in particular within the European Union (EU).

The regulatory framework governing the liability of online service providers in Switzerland consists of the new regulations, as well as general principles and rules embodied in previously existing legislation.

The regulatory context has significantly evolved within recent years in Switzerland without, however, distancing itself from the regulations which previously governed this area or from European regulations,[2] which form a non-binding model for the Swiss rules.

---

1 This is an update of the 2010 edition authored by Veijo Heiskanen, LALIVE SA, Geneva, Switzerland and Philippe Gilliéron, TIMES Attorneys, Lausanne, Switzerland.

2 On 12 December 1999, the European Parliament and the Council of the European Union adopted Directive 1999/93/EC on a Community framework for electronic signatures; This Directive was repealed by Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market (the "Electronic Signatures Directive"). According to the Electronic Signatures Directive, member states of the European Union are to ensure that "advanced electronic signatures," which are defined as electronic signatures that are uniquely linked to the signatory, are (i) capable of identifying the signatory, (ii) created using means that the signatory can maintain under his sole control, (iii) linked to the data to which they relate in such a manner that any subsequent change of the data is detectable and (iv) satisfy the legal requirements of a signature in relation to electronic documents in the same manner as a handwritten signature satisfies those requirements in relation to paper-based documents. On top of "advanced electronic signatures", the Electronic Signatures Directive now provides for "qualified electronic signatures", which is defined as follows (articles 3[12] and 29 and Annex II): "an advanced electronic signature that is created by a qualified electronic signature creation device, and which is based on a qualified certificate for electronic signatures."

The Federal Law of 19 December 2003 concerning the certification services in the field of electronic signature[3] and its statutory instruments[4] govern the conditions which providers must comply with in order to be recognized as providers of data certification service. Article 14 of the Code of Obligations was amended in consequence and now provides that a qualified electronic signature is assimilated to a handwritten signature, subject to any contrary statutory provisions.

It is now possible to file legal submissions by email with the administrative bodies of the Swiss Confederation, and to receive decisions of the bodies in the same way. Subject to certain conditions, appeals before the Swiss Supreme Court also may be filed electronically.[5] Electronic communication in civil, criminal, and debt collection and bankruptcy matters is possible.[6]

Domain Names

Since 1 January 2015, domain names are governed by the Ordinance on Internet Domains (OID).[7] From 1997 to 1 January 2015, Switch, a Swiss foundation of private law, had a monopoly regarding the registration of ".ch" (the only Swiss extension, at that time) domain names. To avoid potential antitrust issues, this situation has changed since 1 January 2015 and Switch is no longer entitled to act as a registrar of ".ch" domain names, but remains responsible to manage the technical aspects of ".ch" domain names. Switch thus stopped selling ".ch" domain names and its former clients are gradually transferring their ".ch" domain names to new registrars, the list of which is available online.[8]

3 *Loi sur la signature électronique*, Law Number 943.03, is currently being revised with the aim of notably simplifying and harmonizing its legal terms as well as creating, in addition to the "advanced electronic signature" and the "qualified electronic signature", the "regulated electronic signature." "Regulated electronic signatures" shall comply with less stringent standards than the "qualified electronic signatures" and shall be available to companies and authorities only (see Message of the Federal Council, 15 January 2014, *Federal Gazette* [*Feuille Fédérale*, FF] 2014 957).

4 *Ordonnance du 3 décembre 2004 sur les services de certification dans le domaine de la signature électronique (Ordonnance sur la signature électronique*, Law Number 943.032*); Ordonnance de l'OFCOM du 6 décembre 2004 sur les services de certification dans le domaine de la signature électronique,* Law Number 943.032.1. These Ordinances are also being revised.

5 *Règlement du Tribunal fédéral du 5 décembre 2006 sur la communication électronique avec les parties et les autorités précédentes* (RCETF), Law Number 173.110.29.

6 *Ordonnance sur la communication électronique dans le cadre de procédures civiles et pénales et de procédures en matière de poursuite pour dettes et de faillite* (OCEI-PCPP), Law Number 272.1; for civil procedure, see article 7 OCEI-PCPP combined with article 130, paragraph 2, of the Code of Civil Procedure (Law Number 272); for criminal procedure, see article 7 of the OCEI-PCPP combined with article 110, paragraph, 2, of the Code of Criminal Procedure (SCCP), (Law Number 312.0); for debt collection and bankruptcy procedure, see article 7 of the OCEI-PCPP, combined with article 33a, paragraph 2, of the Debt Collection and Bankruptcy Act (Law Number 281.1).

7 *Ordonnance sur les domaines Internet*, Law Number 784.104.2.

8 See https://www.nic.ch/reg/en/cm/registrar-list.

The OID also applies to the new domain name ".swiss" granted to Switzerland by the Internet Corporation for Assigned Names and Numbers (ICANN), and available since 7 September 2015.[9] The ".swiss" domain names must serve and promote Swiss interests[10] and, if several candidates compete for the same domain, the latter will be attributed to the candidate providing the best added value for all or part of the Swiss community.[11]

Subject to the Federal Act on Private International Law[12] and the Convention on Jurisdiction and Execution of Judgments in Civil and Commercial Matters,[13] disputes regarding the right to use a domain name are governed by private law. Pursuant to the OID, the registrars must implement a dispute resolution policy,[14] which covers the organization and procedure of an equitable, expeditious, and inexpensive dispute resolution mechanism, inspired by the best practices in the field.[15] The dispute resolution mechanism is not exclusive and does not prevent a party from bringing an action before a competent court.

The OID contains no specific provisions regarding the registrars' liability *vis-à-vis* third parties to the exception that their relation is governed by private law;[16] however, it does provide for the obligation for the registrars to freeze a domain name and to remove the related assignation to a name server in the event where there are founded suspicions that the domain name is used for accessing sensitive information through illegal methods (phisher) or for spreading out malicious software (malware), and if an organ against cybercrime acknowledged by the Federal Office of Communications has requested the freeze.[17]

If no such request for a freeze is submitted, the registrars may proceed *ex officio* under the condition that they lift all measures after a deadline of five working days, unless a request in the sense of the above is submitted in the meantime.[18] In the event of a freeze, the registrars must inform the domain name holder of such freeze by electronic means, requesting the holder to indicate a valid address for correspondence in Switzerland and to decline its identity within 30 days. The

9 See http://www.bakom.admin.ch/themen/Internet/00468/04167/index.html?lang=en. The ".swiss" domains also are governed by the Ordinance of the Federal Department of the Environment, Transport, Energy and Communications on the Internet domain ".swiss" (*Ordonnance du DETEC sur le domaine Internet ".swiss" du 11 août 2015,* Law Number 784.104.253).

10 OID, articles 50 and 53.

11 See http://www.bakom.admin.ch/dokumentation/medieninformationen/00471/index.html?lang=en&msg-id=58618.

12 *Loi fédérale sur le droit international privé*, Law Number 291.

13 *Convention concernant la compétence judiciaire et l'exécution des décisions en matière civile et commerciale* (Lugano Convention), Law Number 0.275.12.

14 OID, articles 10(1) and 14.

15 OID, article 14(1)(e) and (f).

16 OID, article 22.

17 OID, article 15.

18 OID, article 15(2).

domain name is revoked if the holder does not comply within the deadline.[19] The Federal Office of Police renders a decision related to the freeze if, within the 30-day deadline, the holder requests such a decision, having identified itself correctly and indicated a valid address in Switzerland. If the freeze is not confirmed, the registrar lifts it.[20] The registrars must document cases of freezing of domain names and their suppression and present a report on a regular basis. The registrars have no obligation to verify if the applicants or owners of "ch" domain names are entitled to use them.[21]

Surveillance of Access to Internet

The Federal Communication Surveillance Act (FCSA) on the surveillance of postal mail and telecommunications,[22] as well as the related Ordinance,[23] set out the conditions and procedures for the surveillance of physical and electronic mail. According to the FCSA, surveillance can only be conducted in connection with national or international criminal proceedings or for searching and rescuing lost persons,[24] The Code of Criminal Procedure[25] (SCCP), in force since 1 January 2011, specifies that surveillance can only be conducted provided that:

- Serious suspicions exist indicating that the individual concerned may be involved in committing a specific criminal offence (e.g., homicide, assault, unlawful appropriation, robbery, unauthorized obtaining of data, fraud, extortion, criminal mismanagement, threatening behavior);
- The severity of the offence justifies surveillance; and
- The measures taken in connection with the criminal investigation have until then not been effective, such measures cannot be effective without surveillance, or they can be made effective only with undue difficulty.[26]

The FCSA also details the obligations of telecommunications service providers, including Internet service providers. Such obligations[27] may include:

19 OID, article 15(3).
20 OID, article 15(4).
21 OID, article 47(2).
22 *Loi fédérale sur la surveillance de la correspondance par poste et télécommunication*, Law Number 780.1; this law is currently being revised (Message of the Federal Council of 27 February 2013, FF 2013 2379). The revision comprises modifications such as enhancing the scope of application of the law to the search of people who were sentenced to imprisonment, allowing the use of special supervision devices (i.e., IMSI-catchers) or special Internet programs (i.e. GovWare), and extending the preserving period for data from 6 to 12 months.
23 *Ordonnance sur la surveillance de la correspondance par poste et télécommunication*, Law Number 780.11; this Ordinance is currently being revised.
24 FCSA, article 1(1)(a–c).
25 *Code de procédure pénale*, Law Number 312.0; see Message of the Federal Council of 27 February 2013, FF 2013 2379.
26 SCCP, article 269(1)(a–c).

- Transmitting to the competent federal authority, upon request, communications of the individual concerned and related technical information;
- Preserving, for a period of six months, data allowing the identification of users and other related technical information; and
- Safeguarding, *vis-à-vis* third parties, the secrecy of the surveillance and of all related information.[28]

Service providers are entitled to receive a reasonable compensation from the authority that ordered the surveillance for any costs that they may have incurred in this respect.[29] Surveillance may not be authorized other than by a judicial authority.[30]

Liability of Online Service Providers

In General

There is no law in Switzerland specifically addressing the obligations and the scope of liability of online service providers, and the EU Directive on Electronic Commerce does not apply in Switzerland. The "mere conduit" rule embodied in the Directive provides that where the services consist of the transmission in a communication network of information provided by a recipient of the service, or the provision of access to a communication network, the providers may not be held liable except if they initiate the transmission, select the receiver of the transmission, or select or modify the information transmitted.[31] The rationale of this rule is that, if the service providers intervene in the transmission either by selecting the receiver or the message or by modifying the message, they operate as a content provider.

The EU Directive on Electronic Commerce also provides that as regards hosting services, the providers may only be held liable if they have actual knowledge of illegal activity or information and have not acted expeditiously to remove or to disable access to the information.[32] The question whether the "mere conduit"

27 FCSA, article 15.
28 Criminal Code (*Code pénal suisse*), Law Number 311, article 321 *ter*.
29 FCSA, article 16.
30 SCCP, article 272(1).
31 Directive 2000/31/EC of the European Parliament and of the Council on Certain Aspects of Information Society Services, in particular Electronic Commerce, in the Internal Market, 8 June 2000, OJ L178/1, 17, article 12.1, which provides as follows: "[W]here an information society service is provided that consists of the transmission in a communication network of information provided by a recipient of the service, or the provision of access to a communication network, member states shall ensure that the service provider is not liable for the information transmitted, on condition that the provider: does not initiate the communication; does not select the receiver of the transmission; and does not select or modify the information contained in the transmission."
32 Directive on Electronic Commerce, article 14.1.

rule applies to YouTube — an Internet company that offers storage space to host and transmit videos and to search and watch available videos — was addressed by the Tribunal de Grande Instance of Paris in 2012.[33] The plaintiffs argued that YouTube falls within the definition of an editor as it plays an active role on the content of the videos uploaded by its users.

According to the plaintiffs, YouTube notably watches out, *a priori*, for videos with illicit content as its terms and conditions provide that it can remove any video with illicit content, and further promotes the videos with the most attractive content. The Tribunal, however, held that YouTube cannot be compared to an editor, its role being limited to the one of a hosting provider; first, videos are only indicated because of software that runs the search engine and that calculates the statistics of video requests, promoting videos that are most searched, without using them to value the website or for advertisement purposes; and second, although YouTube's terms and conditions indeed allow YouTube to remove any video with illicit content, this stands not for its own benefit but to comply with legal duties bared by service providers, including the removal of any video with patently illegal content. The "mere conduit" rule, therefore, applies to YouTube.

Article 50.1 of the Code of Obligations reads as follows:

". . . where several persons have jointly caused damage, whether as instigators, principals, or accessories, they shall be jointly and severally liable to the damaged party."

The application of this provision does not require the tortfeasors to act jointly; it only requires them to be aware of the fact that their joint behavior may cause damage to a third party.[34] However, to be applicable, the provision requires calls for the following conditions of article 41 of the Code of Obligations to be met with respect to each of the parties:

- Damage;
- Fault;
- Unlawful act; and
- Existence of a causal link between the act and the damage.

In 1999,[35] the Swiss Supreme Court addressed the question of the level of diligence which is required from a printer as regards the content of printed material. It reasoned as follows:

"This means above all that the diligence required from a printer is not the same as that which is required from the author or the editor responsible for the

33 Decision of the Tribunal de Grande Instance of Paris of 29 May 2012, Number RG 10/11205, at pp. 23–25.

34 Decision of the Swiss Supreme Court (ATF) 126 III 167; ATF 115 II 42.

35 ATF 126 III 161 = *Journal des Tribunaux* (JdT) 2000 I, at p. 292.

publication. It is only in the presence of particular circumstances that are brought to its attention that a printer must take measures (. . .)."

This approach is similar to the "mere conduit" European rule, and applies to online service providers since their functions are comparable to those of a printer. Under Swiss law, defensive claims, by contrast to damage claims, may be brought against any participant to the offense, regardless of any possible fault on his/her part.[36] Thus, a person who is not the author of an offensive blog publication but even unknowingly contributes to transmit it may be ordered to stop transmitting it.[37] The "mere conduit" rule is of no relevance in this context.

The Swiss Internet Industry Association (SIMSA), which gathers several online service providers, including Google Switzerland, Switch, Swisscom, RapidShare, and Infomaniak Network, elaborated a Code of Conduct for hosting providers which came into force on 1 January 2013.[38] The Code states that Internet hosting providers have no monitoring obligation over the content stored, processed, and made available by their customers (article 5) but are allowed to partially or completely block access to a website if it receives notice that it appears "very likely" that it concerns illegal content (article 7.1). The SISMA Code of Conduct is not legally binding and only affects SIMSA members. The Swiss parliament adopted a postulate of 29 September 2011 entitled "[T]o give a legal frame to social media,"[39] aiming at determining whether Swiss law adequately deals with the evolution of social media, and sufficiently addresses the liability of the persons who are involved. The analysis is pending.

Under Trade Mark Act

The Trade Mark Act[40] does not contain any specific provisions regarding the obligations and the scope of liability of online service providers. One of the key issues in the context of trade mark law is the liability of an online service provider for the reproduction of a trade mark of a third party on the Internet without consent. The question is whether the mere reproduction can engage the online service provider's liability. According to article 13.2 of the Trade Mark Act:

". . . the holder has the right to prohibit third parties from using signs whose protection is excluded according to article 3(1) of the Trade Mark Act . . . ."

Thus, a trade mark infringement under Swiss law requires the use of the sign by the infringing party. Given this requirement, it appears that only the content provider can be held liable under the Trade Mark Act, to the opposite of the online service provider. Since neither the access provider nor the hosting

36 Civil Code, article 28.

37 ATF 5A_792/2011, paragraphs 6.2 and 6.3.

38 See http://simsa.ch/_Resources/Persistent/baa5c1293ec68a1754e4b5ba2a288faa701fbb92/130201-simsa-cch-public-en.pdf.

39 Postulate Number 11.3912 of 29 September 2011.

40 *Loi fédérale sur la protection des marques et des indications de provenance*, Law Number 232.11.

provider uses the trade mark, such online service providers can indeed be liable only for the content that they themselves distribute on the Internet, if they have actual knowledge of trade mark infringement and, upon obtaining such knowledge, have not acted expeditiously to remove or to disable access to the litigious content.

Under Copyright Act

The relevant issue under copyright law is whether an online service provider is liable if the information that it is providing access to or that it is hosting infringes the copyright of a third party.[41] The applicable principles are similar to those that apply under the Trade Mark Act.

Since 1 July 2008, Swiss copyright law expressly provided that authors have the exclusive right to authorize any communication to the public of their protected works on the Internet or by similar means.[42] In 2014, the European Court of Justice held in the *BestWater* case[43] that posting a link to a copyrighted work which is freely available elsewhere on the Internet does not amount — at least when the work was lawfully made available on the Internet — to a "communication to the public." This reasoning appears to be applicable under Swiss law as well.[44]

Under Unfair Competition Act

The relevant issue under the Unfair Competition Act[45] is whether an online service provider is liable for possible violations by a content provider, e.g., defamatory assertions regarding the content provider's competitors, their products, and their services.[46]

The Act does not require that a competitive relationship exist between the parties for a violation to occur. The Swiss Supreme Court has found on several occasions that the media could be held liable under the Unfair Competition Act for defamatory information they had provided to the public. Sending advertisements in bulk by means of telecommunications (spam) is prohibited in Switzerland.[47] Sanctions for infringement are up to three years of imprisonment or a fine.

41 *Loi fédérale sur le droit d'auteur et les droits voisins*, Law Number 231.1.

42 Copyright Act, article 10(2)c, mirroring article 8, World Intellectual Property Organization Copyright Treaty.

43 Decision of 21 October 2014 in C-348/13.

44 See also François Dessemontet, *La propriété intellectuelle et les contrats de licence* (2011), p. 110 and Philippe Gilliéron, *Les liens hypertextes et le droit privé*, sic ! 2000, 755, p. 763.

45 *Loi fédérale du 19 décembre 1986 contre la concurrence déloyale*, Number 241.

46 Article 2 of the Unfair Competition Act states the general principle to the effect that unfair and unlawful is to be considered all behavior which contravenes the rules of good faith and affects the relationships between competitors or service providers and their clients. See also articles 3–7 of the Copyright Act.

47 Unfair Competition Act, article 3, lit. o.

Summary

Despite numerous amendments to Swiss intellectual property legislation in the past years and the rising awareness of the issue of liability of online services providers, few steps have been taken to clarify the situation and to set clear conditions of online service provider civil liability.

Except for the SIMSA private Code of Conduct for hosting providers, there are no complete regulations specifically addressing the liability of online service providers for infringement of intellectual property rights, unfair competition, or violation of personality rights. In the absence of such specific provisions, the situation must be assessed in light of general legal principles.

Based on an analysis of these principles, it appears that online service providers should face liability under limited circumstances only, in order to not impede the very functioning of the Internet. These are met if the provider intervenes in the contents of the information transmitted or if it is or should have been aware of the infringing contents of a website but has not timely taken appropriate measures.

Privacy and Data Protection

Every click on a user's mouse leaves a trace — an electronic track — that allows, in principle, the user's online service provider to make use of the information. Based on the information, an online service provider can determine who uses the Internet, when, which websites have been accessed, and with whom this information has been exchanged. All of this information enables online service providers to build user profiles.

An online service provider's access to this type of information raises right-to-privacy concerns. These concerns were addressed in the Data Protection Act of 19 June 1992.[48]

While the following discussion will focus on the Data Protection Act, international regulation of data protection also remains relevant. International regulations include the European Convention on Human Rights[49] and the European Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, adopted on 28 January 1981 (Number 108)[50] and amended in 1999. Switzerland is a party to both conventions. While not binding, Council of Europe Recommendation Number R(99)5 of the Committee of Ministers of Member States for the Protection of Privacy on the Internet also is important as it specifically addresses the issue of the protection of online privacy.[51]

48 *Loi fédérale sur la protection des données*, Law Number 235.1.

49 *Convention de sauvegarde des droits de l'homme et des libertés fondamentales*, Law Number 0.101, article 8.

50 *Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel*.

51 Recommendation Number R(99)5 of the Committee of Ministers of Member States for the Protection of Privacy on the Internet, 23 February 1999.

The Data Protection Act applies when data related to individuals or corporations is collected on the Internet, whether by public or private entities. According to its first article, the purpose of the Act is to protect the personality and fundamental rights of individuals and corporations that have been made objects of data collection. Each individual and corporate entity has the right to exercise a certain degree of control over such information and to restrict its processing by third parties.

According to article 2.2, the Data Protection Act does not apply to personal data that is used by individuals for exclusively personal purposes and that is not communicated to third parties. It has been suggested that, based on this exclusion, the Data Protection Act would not apply to a private exchange of e-mails. However, as confirmed by the Swiss Supreme Court, e-mails are, in any event, covered by the secrecy of telecommunications in accordance with article 13 of the Federal Constitution and article 321 *ter* of the Criminal Code.[52] The Data Protection Act embodies several important principles which online service providers must comply with. These are:

- The principle of legality — According to article 4(1), personal data can only be collected in a legal manner. This excludes any unfair or misleading behavior and deception in the collection of data. The principle also effectively bans hidden collection of data.[53]
- The principle of good faith — According to article 4(2), data must be processed in conformity with the principle of good faith. The principle implies that one cannot collect data against the will of the individual concerned. The requirements of transparency and predictability also are linked to this principle and, accordingly, an online service provider should inform Internet users of the possibility of data collection.
- The principle of proportionality — Article 4(2) requires that personal data be processed in conformity with the principle of proportionality. It has been suggested that, based on this principle, personal data may be collected only to the extent that it is necessary to achieve a legitimate goal. There also must be a reasonable relationship between the goal and the means that are used to achieve the goal. The principle applies to the mode and scope of the treatment and the type of personal data that is being used. Based on this principle, certain authors claim that the creation of a database of personal data is prohibited if the website can be freely accessed by the public.
- The requirement of legitimate purpose — According to article 4(3), personal data may not be processed except for a purpose that was identified during the collection of the data, or that is permitted by law, or that is clear from the circumstances. This implies that the purpose of the database must be defined prior to its creation, and that the database may only be used for the defined

52 ATF 126 I 50.

53 For a case of hidden collection of data which was considered as illegal by the Swiss Supreme Court, see ATF 136 II 508 = JdT 2011 II 446, "Logistep."

purpose. Conversely, the principle effectively excludes the collection of data for an undefined purpose.

Article 4(4) provides that the collection of personal data and, in particular, the purposes of data treatment, must be identifiable to the persons concerned. The requirement of identification already expressly existed for the federal authorities when they treat sensible data or personality profiles. This is extended to any type of data and applies to the private sector as well.

Article 4(5) defines the conditions of a lawful consent when such consent is required for personal data treatment. Treatment of personal data can only occur if there is consent or if it is requested by law based on preponderant private or public interest.

Article 5 provides that the correctness of data must be verified and guaranteed. The effect of this requirement depends on the conditions inherent to each data treatment. Although maintaining the requirement of correctness, the article also provides that the person who treats data must take "all appropriate steps permitting deletion or rectification of the incorrect or incomplete data having regard to the purposes for which such data is collected or treated." The amendment imposes an obligation to update data when necessary.

The regime of crossborder data flow was adopted in the additional protocol to the STE 108 Convention and, to a certain extent, to the system of European Directive 95/46/CE. The principle of prohibition to communicate data abroad when personality rights are seriously threatened is maintained. Communication of data abroad is possible when several conditions are satisfied. First, the communication must respect the basic principles of data protection. The data transfer also must be lawful and based on a valid ground, conform to the principle of good faith and proportionality, and must be for a specific purpose and have correct data. Furthermore, communication is generally not possible unless the recipient of the data is subject to legislation ensuring an adequate level of protection. The adequacy of protection should be evaluated in the light of all circumstances relating to the transfer. This implies, in particular, that the recipient is subject to a law offering a protection level similar to Swiss law.

The Federal Data Protection and Information Commissioner holds a list regarding the level of data protection worldwide. By way of examples, China is not deemed to guarantee adequate protection, while the United Kingdom, as well as United States companies adhering to the so-called "US-Swiss Safe Harbor Framework" (the list of United States companies adhering to this framework is available online at https://safeharbor.export.gov/swisslist.aspx), do.

The European Court of Justice[54] recently decided that the "Safe-Harbor" agreement entered into by the European Union and the USA was not compliant with the European Data Protection Directive. This decision was taken in the

54 Judgment of the European Grand Chamber of 6 October 2015, Case C-362/14.

context of a claim related to data transferred by Facebook Ireland to its mother company located in the USA. The claimant, an Austrian resident, wished to prohibit the transfer of his personal data to the United States since, he claimed, United States law and practice did not ensure adequate protection of the personal data against surveillance activities by public authorities.

The claimant referred to the revelations made by Edward Snowden with regard to the activities of the United States intelligence services, in particular the National Security Agency.[55] The European Grand Chamber held that since the Safe Harbor Agreement allowed or indeed forced United States companies such as Facebook to transfer data to United States authorities "to the extent necessary to meet national security, public interest, or law enforcement requirements," without containing any provision related to rules adopted to limit any interference with the fundamental rights of the persons whose data is transferred from the European Union to the United States,[56] it did not comply with the requirements of article 25(6) of the European Data Protection Directive read with the Charter and was invalid.[57]

The Federal Data Protection and Information Commissioner recently indicated that as of the above decision of the European Grand Chamber, the "Safe-Harbor" agreement entered into by Switzerland and the United States is no longer valid either. The Commissioner recommends, as long as a new agreement is not agreed upon, to negotiate specific contractual guarantees when transferring personal data to United States companies pursuant to article 6(2)(a) of the Data Protection Act.[58] A deadline to end by January 2016 has been granted to this effect.

Besides sufficient guarantees permitting to establish an adequate level of protection abroad, communication is possible in the event that the person has expressly given consent to such a crossborder communication or when such communication is indispensable whether in order to protect a preponderant public interest or to establish, exercise, or defend a right through legal action, or if it is necessary to protect the life or physical integrity of the person concerned.

Finally, article 6(2)(g) of the Data Protection Act provides that communication abroad may occur within the same company or group under the same singular management to the extent that the parties are subject to the same data protection rules which guarantee an adequate protection level. Such regulation permits therefore crossborder data communication within the same group of companies.

The Data Protection Act requires that all personal data be protected against any processing that is not authorized by organizational measures or appropriate techniques. This provision is intended to guarantee the confidentiality, availability,

55 Judgment of the European Grand Chamber of 6 October 2015, Case C-362/14, at p. 19.

56 Judgment of the European Grand Chamber of 6 October 2015, Case C-362/14, at pp. 30 and 31.

57 Judgment of the European Grand Chamber of 6 October 2015, Case C-362/14, at p. 33.

58 See http://www.edoeb.admin.ch/datenschutz/00626/00753/00970/01320/index.html?lang=fr.

and integrity of the data.[59] The adequacy of the measures taken must be assessed in light of the purpose for which the data is used, the nature of the data processed, and the available technology. In terms of the ordinance implementing the Data Protection Act, it is provided that:

". . . [a] private person who processes personal data or who makes available an information network assures the confidentiality, availability and correctness of the data to guarantee in an appropriate manner the protection of the data. He protects the data in particular against the risks of (a) accidental or non-authorized destruction; (b) accidental loss of data; (c) technical errors; (d) falsification, theft or illegal use; (e) modification, copying or accessing or other non-authorized processing."[60]

An online service provider should take necessary measures to comply with this provision, such as encryption of the data, authentication of users and messages, or the protection of the databases. On the other hand, as a general rule, no injury to personality has occurred when the individual concerned has given public access to the data and has not expressly objected to its processing.[61] The Data Protection Act specifically provides that injury to personality constitutes a wrong unless it is justified by the victim's consent, an important private or public interest, or by law.[62]

A legal action for injury to personality must be brought pursuant to articles 28 *et seq*. of the Civil Code. The plaintiff may require, in particular, the correction of the data or its destruction, or the prohibition of its communication to a third party. If the accuracy of the data cannot be established, the plaintiff may require that it be clearly indicated that the accuracy of the data is subject to dispute. The plaintiff also may require that any correction of the data or its destruction, or an indication of its disputed character, be communicated to third parties.[63]

Communications and Defamation

In General

The relevant provisions in regard to communications and defamation are articles 28 and 322 *bis* of the Criminal Code. Article 28 provides as follows:

- When an infringement is made and consummated in the form of publication by the media, the author alone is punishable, in accordance with the following provisions.
- If the author cannot be discovered or if he cannot be brought before a court in Switzerland, the editor in charge is punishable by virtue of article 322 *bis*. In

59 Data Protection Act, article 7(1).
60 *Ordonnance du Conseil fédéral relative à la loi fédérale sur la protection des données*, Law Number 235.11, article 8.
61 Data Protection Act, article 12(3).
62 Data Protection Act, article 13(1).
63 Data Protection Act, article 15.

the absence of an editor, the person responsible for the publication in question is punishable by virtue of the same article.

- If the publication took place without the knowledge of the author or against his will, the editor or, in his absence, the person responsible for the publication, is punishable like the author of the act.
- The author of a truthful report dealing with a matter subject to public discussion or official statements of authorities does not incur any criminal liability.

Article 322 of the Criminal Code provides:

"A person responsible within the meaning of article 28, paragraphs 2 and 3, of an infringing publication shall be sentenced to imprisonment or a fine, if he intentionally did not object to the publication. If he acted out of negligence, the punishment shall be an arrest or a fine."

There is no case law specifically addressing the criminal liability of online service providers. However, pursuant to a request made by the Federal Police, the Federal Office of Justice delivered in 1999 a legal opinion on the criminal liability of Internet access providers.[64] The Federal Police have issued a separate opinion on hosting providers" criminal liability.[65] These two opinions are discussed separately below.

Opinion of Federal Office of Justice on Access Providers

The Federal Police in its request formulated the issue as follows:

"Can an Internet service provider, in its function of providing access for its clients to foreign websites, be qualified as the person responsible for the publication, within the meaning of article 28, paragraph 2, of the Criminal Code?"

Based on this formulation of the question, the Federal Office of Justice assumed that the following conditions prevailed:

- The online service provider is aware of the infringing contents of the information on the website (either through authorities or private parties);
- The hosting provider and the web server are located abroad;
- The access provider's role is limited to that serving as a "mere conduit" of Internet traffic; and
- The decision to access the website is the sole responsibility of the client.

The Federal Office of Justice noted that, on 1 April 1998, the scope of the provisions of the Criminal Code regarding the media's criminal liability were

64 *La responsabilité pénale des fournisseurs de services Internet*, 24 December 1999 ("Legal Opinion"); see https://www.bj.admin.ch/dam/data/bj/sicherheit/gesetzgebung/archiv/netzwerkkriminalitaet/position-fedpol-f.pdf

65 Legal Opinion, at pp. 5 and 6.

extended to apply to all media, including radio, television, and other new media.[66] Based on positions taken by the legislature and other government agencies, including the Federal Council,[67] the Federal Office of Justice concluded that the Internet should be considered as one of these new mass media within the meaning of article 55 of the Federal Constitution.[68]

The Federal Office of Justice then considered the question of whether an access provider can be held liable under criminal law for the contents of a website under article 28 of the Criminal Code.

As a matter of principle, the author of a publication is exclusively liable for its contents.[69] For criminal liability to extend to others than the author, such as to an online service provider, the latter must be in a position to exercise a certain degree of control over the contents of the materials published on a website.[70]

As pointed out by the Federal Office of Justice, a hosting provider is normally in a much better position than an access provider to exercise such control.[71] An access provider's liability can only be engaged as "a person responsible for the publication"[72] if the author of the publication in question, or the content provider, cannot be located.[73] An access provider's liability, if any, for infringing materials published on a website can thus be only subsidiary.[74]

The Federal Office of Justice recognized that, given an access provider's role and capability to exercise control over the contents of a website, the likelihood of its becoming criminally liable for the contents is limited. However, such liability cannot be excluded *a priori*, as an access provider, like any other person, can be held liable for its own wrongful behavior.[75] Whether or not an access provider has in fact incurred such criminal liability depends on the criteria enumerated in article 322 *bis* of the Criminal Code, which includes the requirement of fault.

66 Legal Opinion, at pp. 5 and 6.

67 FF 1996 IV 558.

68 Legal Opinion, at pp. 5–9. While the classification of the Internet as one of the mass media has been questioned by some authors, the position adopted by the Federal Office of Justice seems to represent the view of the majority of the Swiss doctrine. Article 55 *bis* of the former Federal Constitution has been modified and replaced by article 93 of the new Federal Constitution, which entered into force on 1 January 2000.

69 Criminal Code, art 28(1).

70 Legal Opinion, at p. 15.

71 Legal Opinion, at p. 16.

72 SCCP, article 28(2).

73 Legal Opinion, at pp. 15–17.

74 Legal Opinion, at pp. 15–17.

75 Legal Opinion, at p. 17. This does not mean that its liability is excluded. Indeed, in the *PTT Case*, the Swiss Supreme Court held that the Federal Post bore accessory liability for having allowed the transmission of pornographic material over telephone lines (ATF 121 IV 109).

Article 322 *bis* of the Criminal Code, read together with article 28(2), requires an access provider to have purposely refrained from preventing users from accessing the infringing site. This requirement implies that the access provider is aware of the existence of the infringing site, and that it has an obligation to prevent Internet users from accessing it.[76] Awareness can be inferred when a law enforcement authority has brought the potentially infringing contents of a website to the access provider's attention.

While the possibility exists that a court may not uphold the criminal charge brought by a law enforcement authority, the fact that an official investigation has been opened into the legality of the materials published on a website should provide a basis for an access provider to assume that there is at least sufficient doubt about the legality of the materials.[77]

On the other hand, information obtained through individuals or the media should normally not be sufficient to establish awareness or to create an obligation to prevent users from accessing the site in question. In the view of the Federal Office of Justice, this approach also reduces the risk of "private censorship."[78]

As noted by the Federal Office of Justice, the criminal intention of an access provider, as required by article 322 *bis*, can only rarely be established.[79] If at all, an access provider can normally be held liable only for negligence, which raises the question of the level of due diligence that can reasonably be expected from an access provider. According to the general principle, a person who creates a dangerous situation is required to take any reasonable measures to prevent injury or damage from occurring as a result of the situation.[80] This means that an access provider is required to take any reasonable measures that may be available to prevent Internet users from accessing the infringing website.[81]

However, in the view of the Federal Office of Justice, an access provider may be liable for negligence only if a law enforcement authority has brought the contents of the infringing website to the access provider's attention, if such information is concrete and reliable, and if no action is taken.[82] Thus, access providers are likely to be found liable only under exceptional circumstances.[83]

As article 28 of the Criminal Code requires that the infringement be made "in the form of publication by the media," it has been suggested that the provision does not apply to e-mails that are normally exchanged privately or between a

76 Legal Opinion, at p. 19.
77 Legal Opinion, at p. 20.
78 Legal Opinion, at p 20.
79 Legal Opinion, at p. 21. This may happen, e.g., in instances where an access provider adopts a corporate policy after being notified by a law enforcement authority not to block access to a particular website.
80 Legal Opinion, at p. 23.
81 Legal Opinion, at p. 23.
82 Legal Opinion, at p. 25.
83 Legal Opinion, at p. 25.

limited number of individuals. It is arguable, however, that an e-mail sent to recipients on a mailing list can be considered to be a "form of publication" within the meaning of the legal provision, as this involves the distribution of the message to a larger indefinite number of individuals. Similar considerations apply to messages exchanged on electronic discussion *fora*.

Although websites are generally publicly accessible and thus may be considered to be a "form of publication" under article 28, this provision does not cover all crimes committed over the Internet in the form of publication. In a decision rendered on 10 August 1999, the Swiss Supreme Court held that article 27 did not apply to article 135 (representation of violent crime), article 197(3) (hard pornography), and article 261*bis* (racial discrimination) of the Criminal Code.[84]

The Supreme Court stated that articles 28 and 322 *bis* were to be held *leges speciales* as they permit the sentencing of each intermediary as the main author and not merely as an accessory. When these provisions do not apply, an access provider's liability must be examined according to the general rules, i.e., article 25 of the Criminal Code, which deals with the culpability of an accessory.[85] Here, it is required as well that the access provider's attention has been drawn to the criminal contents of the website.[86] However, as one cannot become an accessory by negligence, it is highly unlikely that an online service provider could be found liable in instances where articles 28(2) and 322 *bis* of the Criminal Code do not apply.

The key issue is thus whether an access provider should be considered to be a subsidiary author[87] or an accessory.[88] If an access provider can only be held liable as an accessory, the controlling precedent would be the *PTT* case mentioned above. It should be noted, however, that certain authors have questioned whether the principle stated in *PTT* can be applied to an access provider.

First, under *PTT*, the activity of an accessory must be unlawful; this cannot be the case with respect to an access provider who serves as a mere conduit of information. In addition, the hotline at issue in *PTT*, which had been tolerated by the Federal Post, had generated substantial revenues to the latter. This is normally not the scenario in the case of an access provider, as access charges relating to a particular infringing website are unlikely to have a substantial impact on the access provider's revenues.

The Federal Office of Justice's view on the scope of an access provider's criminal liability has been contested by some who argue that an access provider does not fall

84 ATF 125 IV 206; for criticism of this case, see Franz Riklin, *Kaskadenhaftung — quo vadis?*, Medialex 2000, p. 199; Schleiminger and Mettler, *Note*, Pratique juridique actuelle 1039, 2000.

85 Legal Opinion, at pp. 26 and 27. According to article 25 of the Criminal Code, "[t]he punishment may be attenuated...for those who have intentionally assisted in the commitment of a crime or a delict".

86 Legal Opinion, at p. 27.

87 Criminal Code, article 28(2).

88 Criminal Code, article 25.

under article 28(2) of the Criminal Code in terms of being "a person responsible for the publication." An access provider cannot be considered "responsible" for the publication of the materials, as it only provides access to websites, without having any influence over the information transmitted. According to this view, holding an access provider liable for the contents of a website would be tantamount to holding a newsstand liable for the contents of the newspapers it sells. The Federal Office of Justice is simply looking for an intermediary that can be held ultimately liable, whether or not there is any fault involved.

Opinion of Federal Police on Hosting Providers

As noted above, the Legal Opinion of the Federal Office of Justice deals primarily with the criminal liability of access providers. To complement this opinion, the Federal Police issued in 2000 a further legal opinion that addresses the criminal liability of hosting providers (the "Federal Police Opinion").

In the view of the Federal Police, the rules governing the criminal liability of hosting providers are generally the same as those that apply to access providers. Consequently, pursuant to article 28(2) of the Criminal Code, a hosting provider can be held liable for the contents of a website only on a subsidiary basis, i.e., only if the content provider is not based in Switzerland and cannot be brought before a Swiss court.[89]

As in the case of the access provider, awareness of the contents also is required to establish the hosting provider's liability. The Federal Police acknowledges that, given its function, a hosting provider cannot be expected to inspect the contents of all data hosted.[90] However, under certain specific circumstances, a hosting provider may have reason to inspect such data, e.g., based on information that it has obtained when entering into a contract with the website owner.[91]

As a hosting provider has a contractual relationship with the website owner and as the volume of information that it has under its control is much less than in the case of the access provider, a hosting provider should take into account not only any information that may have been provided to it by law enforcement authorities, but also any information that has been communicated to it by private individuals.[92] This means that, unlike an access provider, a hosting provider can be expected to inspect, at least on a sample basis, the contents of the data that it is hosting if the contents appear to be suspect.[93]

89 Federal Police Opinion, at p. 6.

90 Federal Police Opinion, at pp. 6 and 7.

91 Federal Police Opinion, at p. 7. This obligation extends to FTP servers only to the extent that files are readable by standard computers.

92 Federal Police Opinion, at p. 7.

93 Federal Police Opinion, at p. 13. The Federal Police also noted in their opinion that the webmaster of an Internet Relay Char Server does not bear any criminal liability, as the transmission of the data is too transient to be relevant from a criminal law point of view. Federal Police Opinion, at p. 8.

The Federal Police stressed that its opinion was limited to services provided to the public. Consequently, online service providers bear no responsibility for contents in zones of the Internet that are not accessible to the public.[94] In addition, given that e-mails and Internet telephony are covered by the secrecy of telecommunications, online service providers have no right to access them without official authorization.[95] The Federal Police also noted that, while online service providers have the duty to take reasonable measures to prevent users from accessing infringing data, they have no legal obligation to "incriminate" website owners by communicating to law enforcement authorities information about potentially infringing sites.[96]

The controversy that arose from these opposed positions was reinforced by a branch of online service providers who rejected the conclusions formulated by the Federal Department of Justice and Police as above mentioned. In their October 2001 legal opinion, the online services providers' experts arrived at conclusions essentially different from those of the Federal Department of Justice and Police. Under political pressure, the head of the Federal Department of Justice and Police formed an expert commission on 22 November 2001 which was appointed to examine which measures may be applied in order to prevent and to sanction offences committed via Internet. Within this framework, the commission was charged to examine the issue of regulation of criminal liability in the Internet field.

In December 2004, the Federal Government issued for consultation two pre-bills of amendments to the Criminal Code and Military Criminal Code, accompanied by an explanatory report.[97] The pre-bill concerned provider criminal liability. In essence, it was admitted that general provisions of the Criminal Code in relation to offender and complicity are applicable to providers who actively participate in commission of offences.

An access provider was to be punished if, knowing or subsequently establishing that information subject to criminal liability was transmitted through its website, the access provider failed to prevent usage of the information or failed to inform the criminal prosecution authorities. On the other hand, the access provider remained unpunished if his actions were limited to the provision of automatic access to the Internet.

The vast majority of the circles concerned approved the will to intensify the combat against offences committed via electronic media. The provisions envisaged in the pre-bill concerning access providers have, however, given rise to very contrasting reactions. Finally, the consultation showed general determination to regulate in an express manner the criminal liability of providers. However, it

94 Federal Police Opinion, at pp. 13 and 14.
95 Federal Police Opinion, at p. 14; ATF 126 I 50.
96 Federal Police Opinion, at p. 14.
97 See https://www.bj.admin.ch/dam/data/bj/sicherheit/gesetzgebung/archiv/netzwerkkriminalitaet/vn-ber-f.pdf.

was admitted unanimously that the proposed amendment was going to cause new uncertainties. In 2008, the Federal Council[98] recommended to the Parliament to abandon any explicit regulation of the criminal liability of the providers. Even if legislation does not contain any specific rules concerning criminal liability of providers, it considered that it is possible to find valid solutions relying on media criminal law and general principles.

In a decision of 2007,[99] the Swiss Supreme Court examined the conditions under which an online chat forum operator may be held criminally liable for publishing unlawful information. The case concerned a forum where videos were posted inciting terrorist acts against westerners. The forum operator was found liable for having made available an online platform for exchange of content and not just for having omitted to withdraw unlawful content. According to the Court, a forum operator is intrinsically linked to the risk that unlawful contents are placed on the forum.[100] In such case, the operator has the obligation to delete contentious content pursuant to the unwritten principle that whoever creates a danger is to take the necessary steps to avoid the consequences thereof.

As the operator approved the content and the opinions conveyed by the videos, he was convicted of offense of supporting a criminal organization: the Swiss Supreme Court considered that his participation went beyond helping and assisting and, therefore, he had acted as a co-author and not as an accomplice. In the recitals of the decision, the Court excluded the obligation to permanently control the legality of the external contributions. However, once the site manager is informed, whether himself or through a third party, of the existence of unlawful content, he has the duty to withdraw it.

Fraud and Internet Crime

Gambling

According to article 5 of the Federal Law on Games of Chance and Gambling Houses,[101] the use of an electronic communication network such as the Internet for purposes of games of chance is prohibited. Articles 55 and 56 of the Law specify the criminal sanctions resulting from the infringement of its provisions.

Drugs

According to article 27 of the Federal Law on Drugs and Medical Appliances,[102] distance sale of drugs is, in principle, prohibited. However, distance sale can be authorized by the competent canton under specific criteria defined in the law and

98 See https://www.bj.admin.ch/dam/data/bj/sicherheit/gesetzgebung/archiv/netzwerkkriminalitaet/ ber-br-f.pdf.

99 ATF 6B_645/2007; ATF 6B_650/2007.

100 ATF 6B_645/2007; ATF 6B_650/2007.

101 Law Number 935.51. See also ATF 2C 312/2007.

102 *Loi fédérale sur les médicaments et les dispositifs médicaux*, Law Number 812.21.

based on guidelines provided by the Federal Council.[103] In addition, article 31 of the Law provides that the advertisement of drugs is permissible only to the extent that it is addressed exclusively to medical professionals or concerns drugs that are not subject to prescription.

Alcohol

According to article 42b(3), lit. a, of the Federal Act on Alcohol,[104] the advertisement of alcoholic beverages is prohibited on radio and television. However, there is no mention of the Internet. As the Internet is a new medium of communication that has novel features clearly distinguishing it from the radio or the television, it is unclear that advertisement of alcohol on the Internet is prohibited in Switzerland. The Federal Act on Alcohol is currently being totally revised.[105]

Jurisdiction and Applicable Law regarding Online Service Providers

Civil Matters

Jurisdiction

The jurisdiction of Swiss courts over foreign parties is regulated by the Federal Private International Law Act and the Convention on the Jurisdiction and Execution of Judgments in Civil and Judicial Matters.[106] According to the Act's general principles governing the jurisdiction of Swiss courts in actions based on tort (*actes illicites*), if the defendant has no domicile in Switzerland or is not habitually resident in Switzerland or, in the case of a juridical person, has no place of business in Switzerland, action can be brought before a Swiss court if the act occurred or its effect was felt in Switzerland.

On the basis of this principle, a Swiss court may assert jurisdiction over a foreign online service provider whose liability can be established on the basis of the rules discussed above, to the extent that the effects of the infringement are felt in Switzerland, e.g., if the injured party is a Swiss individual or legal entity. The mere fact that the website is accessible in Switzerland is thus not sufficient to establish jurisdiction.

Jurisdiction over intellectual property matters is regulated by article 109 of the Federal Private International Law Act, which reads as follows:

"Swiss courts of the defendant's domicile have jurisdiction to entertain actions pertaining to the validity or registration in Switzerland of intellectual property rights.

103 Federal Law on Drugs and Medical Appliances, article 27(2)–(4).
104 *Loi fédérale sur l'alcool*, Law Number 680.
105 See http://www.eav.admin.ch/dienstleistungen/00636/index.html?lang=en.
106 Federal Private International Law Act, Law Number 291, article 129(1); Lugano Convention, article 5(3).

"(1) When a defendant does not have a domicile in Switzerland, these actions shall be brought before the Swiss courts at the commercial office of the representative recorded in the register or, in the absence of such representative, before the courts at the place where the authority keeping the register has its office.

"(2) Actions pertaining to the violation of intellectual property rights shall be brought before the Swiss courts at the defendant's domicile or, in the absence of a domicile, at the defendant's habitual residence. Swiss courts at the place where the act or the result occurred also have jurisdiction, and for actions pertaining to the operation of the place of business in Switzerland, the action must be brought before the courts at the place of business."

As regards unfair competition, Swiss courts have jurisdiction if the Swiss market was affected by the litigious act.[107]

Applicable Law

The applicable law determines, in particular, the capacity of the tortfeasor to be held liable for a wrongful act, the conditions and the extent of liability, as well as the individual to be held liable. Rules of conduct and safety that prevail at the *situs* of the tort must be taken into account.[108]

According to the general rule embodied in article 132 of the Private International Law Act, the parties may, at any time after the event that caused the damage, agree to apply the law of the forum. In the absence of such an agreement, when a tortfeasor and the injured party do not have their habitual residence in the same state, the action is governed by the law of the state in which the tort was committed.[109] However, if the effect of the act was felt in another state, the law of that state is applicable if the tortfeasor should have foreseen that the act would have its effect in that state.

The law applicable to intellectual property right infringements is defined in article 110 of the Private International Law Act, which provides that these rights are governed by the law of the state on which the action is based, i.e., the law of the state on the basis of which protection is sought. If the action is based on tort, the parties may agree, after the infringement took place, that the law of the forum (i.e., Swiss law) applies. Actions based on unfair competition are governed by the law of the state whose market is affected by the litigious behavior. If the act affects exclusively the business interests of a particular competitor, the law of the seat of the injured company applies.[110] Article 139 of the Private International Law Act provides that an action based on injury to personality by media, including the press, radio, television, or any other public

107 Private International Law Act, article 129(1). For a case where Swiss jurisdiction was denied in the matter of an online crossborder advertising campaign, see decision by the Geneva Court of Justice Number ACJC/1488/2014 of 4 December 2014.

108 Private International Law Act, article 133(2).

109 Private International Law Act, article 133(2).

110 Private International Law Act, article 136.

medium of information, is governed by the law chosen by the injured party from among the following:

- The law of the state in which the injured party has its habitual residence, provided that the tortfeasor should have expected that the effect of the act would take place in that state;
- The law of the state in which the tortfeasor has its place of business or its habitual residence; or
- The law of the state in which the effect of the injury takes place, provided that the tortfeasor should have expected that the effect would take place in that state.

According to article 139(3) of the Private International Law Act, the above rules also apply to injury to personality as a result of the processing of personal data, as well as to any limitation placed on the exercise of the right of access to personal data.

Criminal Matters

The jurisdiction of Swiss courts over foreign nationals in criminal matters is defined in the Criminal Code. Article 3(1) of the Code confirms the principle of territoriality, to the effect that the Code applies to anyone who has committed a crime or an offense in Switzerland. The principle is further specified in article 7(1) of the Code, which provides that a crime or a delict is deemed to have been committed both in the place where the author acted and where its effect took place.

When a crime is committed on the Internet, both the Swiss legislature and case law have adopted the view that "the place where the author acted" is the place where the data was uploaded and not the location of the service provider that transmitted this information.[111] In any event, the effects of the crime must be felt in Switzerland. Consequently, the mere fact that the infringing website is accessible in Switzerland is not sufficient to establish jurisdiction.

According to article 31 of the Code of Criminal Procedure (SCCP), the competent Swiss jurisdiction to investigate and adjudicate over a criminal offence is the jurisdiction of the place where the author acted. If the place where the effect of the act took place or was intended to take place is solely in Switzerland, the local Swiss court is competent. Article 35 of the SCCP regulates the jurisdiction of Swiss courts' jurisdiction with respect to acts committed by media: if the criminal act is committed in Switzerland, the forum of the place where the media company has its place of business is competent.

111 Christian Schwarzenegger, *Der räumliche Geltungsbereich des Strafrecht in Internet*, Revue pénale suisse, 2000, pp. 117 *et séq*; Philippe Weissenburger, *Zum Begehungsort bei Internet Delikten*, Revue suisse des juristes bernois, 1999, pp. 703 *et séq*.

If the author is known and resides in Switzerland, the local Swiss court of the residence of the author also is competent. If the competent forum cannot be determined on the basis of these rules, the forum of the place where the product is distributed is competent; if there are several such places, the place where the investigation was first opened is considered to be competent.

When the editor of a website regularly updates the site, the identification of the "author" should be relatively straightforward, as article 322(2) of the Criminal Code requires the editor of a periodical to provide contact details. However, it seems unlikely that this requirement will be generally respected on the Internet. In these circumstances, the domain name holder should be considered to be the "media company" within the meaning of article 35 of the Code.

The domain name holder should be easily identifiable with the assistance of the WHOIS database of the domain name registrar. If the author cannot be identified on this basis, the jurisdiction of the place where the product has been distributed is competent. The only way to prevent a situation from arising where several cantons assert jurisdiction over one and the same website would seem to be the rule that the jurisdiction of the place where the effect of the act was felt, i.e., the residence of the victim, is considered competent.

Conclusion

A regulatory framework exists in Switzerland for the provision of online services. As there is, as yet, little case law specifically addressing the liability of online service providers for intellectual property right infringement or the scope of their general civil and criminal liability, the existing regulatory framework creates a relatively unpredictable environment for the conduct of online business.

The field is likely to remain subject to significant regulatory developments over the next few years, as the legislature seeks to catch up with rapid technological developments and has not yet taken the opportunity to clarify the legal situation.