9-1-2010

Enforcing Intellectual Property Rights by Diminishing Privacy: How the Anti-Counterfeiting Trade Agreement Jeopardizes the Right to Privacy

Alberto Cerda Silva
Universidad de Chile, albertocerdasilva@gmail.com

ENFORCING INTELLECTUAL PROPERTY RIGHTS BY DIMINISHING PRIVACY: HOW THE ANTI-COUNTERFEITING TRADE AGREEMENT JEOPARDIZES THE RIGHT TO PRIVACY[1]

Alberto Cerda Silva[2]

ABSTRACT

Enforcing the law in the digital environment is one of the main challenges of the Anti-Counterfeiting Trade Agreement (ACTA). In order to enforce the intellectual property law, unlike previous international agreements on the matter, ACTA attempts to set forth provisions concerned with privacy and personal data. Special provisions refer to law enforcement in the digital environment; ACTA would require the adoption of domestic law to allow identifying supposed infringers and, consequently, the collaboration of the online service providers (OSPs) with rights holders. However, those provisions raise some human rights concerns, particularly as related to the right to privacy of Internet users and the right to protection of their personal data.

This paper describes the ACTA provisions on the rights to privacy and personal data protection and compares them with domestic privacy law in the context of intellectual property enforcement, particularly those of the United States (U.S.) and the European Union (EU). The underlying hypothesis of this paper is that the ACTA provisions do not harmonize the domestic laws in force, instead it creates a new standard, beyond any domestic law; the full implementation of those provisions would require modifications in the domestic law, which seriously undermines the right to privacy and

---

[1] At the time this paper was researched and written, the July 1, 2010 draft of ACTA was the most recent draft of the text. Any references to "the most recent text" and related analysis refer to the July 1, 2010 draft. After this paper was submitted for publication, a new draft of ACTA was leaked on Aug. 25, 2010. This paper may be revised by the author to reflect changes made by the Aug. 25, 2010 draft text.

[2] Professor, University of Chile Law School.

protection to personal data. Therefore, this paper calls for some modifications in the current text of ACTA in order to reach an adequate balance between intellectual property enforcement and the aforementioned rights to privacy and personal data protection.

I. BACKGROUND

Globalization, digitalization, and the Internet have been the main

challenges for intellectual property since the turn of the century. Globalization has reduced the cost of transportation and communication across the world;[3] the digitalization of content has facilitated and increased the flow of copyrightable works;[4] and, the Internet, which is the paradigm of global services, has allowed the cross-border transfer of digital works in seconds. As a result of those phenomena, creating and maintaining an adequate protection for intellectual property rights has required several modifications of the law on the international level, especially in copyright.

International instruments on intellectual property have focused their efforts on achieving the harmonization of domestic laws by adopting common standards related to the scope, the rights, the duration, and limitations of intellectual property rights. However, to some extent, two issues have been postponed in the international *fora*: the enforcement of those rules and its adequacy to the digital environment. These are the main topics addressed by ACTA with the goal of addressing the counterfeiting and piracy of goods that affect commercial interests.

This paper analyzes the provisions of ACTA that unsuccessfully attempt to balance the protection of intellectual property rights and the fundamental rights of users, especially those related to the right to privacy and the right to protection of personal data.

II. ACTA'S PURPOSES AND PRIVACY PROVISIONS

According to statements of governments that have taken part in the negotiation of ACTA, the initiative aims to establish international standards for enforcing intellectual property rights to target more efficiently the increasing problem of counterfeiting and piracy that significantly affects commercial interests, rather than the activities of common people.[5] However, the analysis of the privacy provisions of ACTA shows a different

---

3 JOSEPH STIGLITZ, GLOBALIZATION AND ITS DISCONTENTS 27 *et seq*. (2002).

4 NICHOLAS NEGROPONTE, BEING DIGITAL (1995) (explaining the inadequacy of current intellectual property regulation, originally designed to protect analog works, to protect digital works). The cause of this inadequacy would be the whole difference between atoms and bits.

5 *See*, G8 Toyako Declaration on World Economy, July 8, 2008, ¶ 17, *available at* http://www.america.gov/st/texttransenglish/2008/July/20080708102050bpuh0.9821131.html (last visited Sept. 20, 2010). G8 includes the government of Canada, France, Germany, Italy, Japan, Russia, the United Kingdom, and the United States. *See also* Press Release, European Commission, Anti-Counterfeiting Trade Agreement: European Commission Welcomes Release of Negotiation Documents (April 21, 2010), *available at* http://trade.ec.europa.eu/doclib/press/index.cfm?id=552 (expressing that ACTA's purpose is to "address large-scale infringements of intellectual property rights" and "no means lead to a limitation of civil liberties or to 'harassment' of consumers.").

concern, and they seem to focus more on enforcing the law against citizens rather than against criminal organizations and/or serious crime.

The negotiations of ACTA have not taken place in any multilateral *fora*, such as the World Trade Organization (WTO) and the World Intellectual Property Organization (WIPO), but they have involved several countries. In fact, currently, the negotiations include Australia, Canada, Japan, Mexico, Morocco, New Zealand, Singapore, South Korea, Switzerland, the U.S., and the European Union.

From 2008 to August 2010, there have been ten rounds of negotiations, which have been conducted mainly in secret. Only after enormous pressure from civil society organizations and the European Parliament[6] was there an official public release of the proposed text of the agreement, after the 8th round, in April 2010.[7] Unfortunately, in spite of the requirement of transparency, there has not been any new public release of the negotiations. However, there are leaked versions of the draft of the agreement, one before and another after the official public release, in January and July 2010, respectively.[8] All those documents permit viewing a mosaic of the progress during the negotiations, particularly the leaked versions of the agreement, since they, unlike the official release, include the positions of negotiators by country and uncensored text of footnotes. Given its high verisimilitude and updated content, this paper is based on the last consolidated text available from July 1, 2010; therefore, all the references to the ACTA text here and elsewhere are to that document, except as otherwise mentioned.

The current text of ACTA is structured in six chapters that include initial provisions and definitions,[9] the proposed legal framework for

---

6 Resolution of 10 March 2010 on the Transparency and State of Play of the ACTA Negotiations, EUR. PARL. DOC. P7_TA-PROV(2010)0058, *available at* http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2010-0058+0+DOC+XML+V0//EN&language=EN.

7 Anti-Counterfeiting Trade Agreement, Consolidated Text Prepared for Public Release Public Predecisional/Deliberative Draft: April 21, 2010, PIJIP IP ENFORCEMENT DATABASE, http://sites.google.com/site/iipenforcement/acta (follow "Official Consolidated ACTA Text Prepared for Public Release, April 21, 2010" hyperlink) [hereinafter ACTA Draft – Apr. 21, 2010]

8 Before the 7th round, in January 2010, was released the first leaked version of the agreement. *See*, Anti-Counterfeiting Trade Agreement, Consolidated Text, Informal Predecisional/Deliberative Draft, January 18, 2010 [hereinafter ACTA Draft – Jan. 18, 2010]. Immediately after the 9th round, in July 2010, was released the second one. *See* Anti-Counterfeiting Trade Agreement, Consolidated Text, Informal Predecisional/Deliberative Draft, 1 July 2010 [hereinafter ACTA Draft – Jul. 1, 2010]. All versions, official and leaked, are available at the PIJIP IP Enforcement Database, http://sites.google.com/site/iipenforcement/acta.

9 ACTA Draft – July 1, 2010, *supra* note 8, Ch. One: Initial Provisions and Definitions, arts. 1.1 to 1.X.

enforcement of intellectual property rights,[10] norms about international cooperation,[11] enforcement practices and mechanisms,[12] an institutional arrangement,[13] and final provisions related to the effects of the agreement.[14] For purpose of this paper, it is necessary to explain with some detail those norms related to the legal framework for enforcing the law, which includes provisions on civil liability, border measures, criminal enforcement, and special measures related to technological enforcement of intellectual property in the digital environment.

In relation to civil enforcement, ACTA requires parties to have available civil procedures to enforce rights, including provisions about injunctions, damages, other remedies, access to information related to infringement and infringers, and provisional measures.[15]

The section related to border measures requires the adoption of certain mechanisms by parties when goods are suspected of infringing intellectual property rights, except in case of *di minimis* infringement.[16] Those measures can be adopted under application of the rights holders and also *ex officio*.[17] Parties shall provide safeguard measures, procedures to determine infringement and remedies, reasonable enforcement fees, and the disclosure of information about infringements and infringers.[18]

Related to criminal enforcement, ACTA attempts to conceptualize criminal offenses, to extend liability to legal persons and inciting conducts, and to adopt criteria for penalties and sanctions.[19] As to these points, the draft still shows an important lack of agreement among the different proposals. ACTA includes provisions about seizure, confiscation/forfeiture, and destruction of suspected counterfeit (trademark) or pirated (copyright) goods.[20] Finally, ACTA requires parties to allow *ex officio* criminal enforcement and to ensure the rights of the defendants and third parties.[21]

The section about technological enforcement of intellectual property in the digital environment[22] is by far the most innovative of the instrument, since several of the issues raised by those provisions never have been

---

10 *Id.* Ch. Two: Legal Framework for Enforcement of Intellectual Property Rights, arts. 2.X to 2.18.
11 *Id.* Ch. Three: International Cooperation, arts. 3.1 to 3.3.
12 *Id.* Ch. Four: Enforcement Practices, arts. 4.1 to 4.5.
13 *Id.* Ch. Five: Institutional Arrangement, arts. 5.1 to 5.3.
14 *Id.* Ch. Six: Final Provisions, arts. 6.1 to 6.7.
15 *Id.* arts. 2.1 to 2.5.
16 *Id.* art. 2.X.
17 *Id.* art. 2.7.
18 *Id.* arts. 2.9 to 2.13.
19 *Id.* arts. 2.14 and 2.15.
20 *Id.* art. 2.16.
21 *Id.* art. 2.17.

regulated in previous international instruments on intellectual property, not even the WIPO Internet Treaties.[23] Basically, this section includes provisions about the limitation of liability related to online material for online service providers and the protection for effective technological measures and rights management information. This section, which seems drafted as an updated version of the Digital Millennium Copyright Act (DMCA),[24] still shows an evident absence of agreement among the parties. In fact, by the tenth round of negotiations, almost all the articles are in brackets, several of them have different proposals, and the section contains more footnotes than any other.

Different from previous international agreements on intellectual property, ACTA includes explicit references to privacy and data protection. Neither the Berne Convention nor the Paris Convention, which are the main international instruments on copyright and patents, makes any reference to privacy or data protection. By its part, the TRIPS Agreement only refers to them indirectly, by allowing WTO members to provide that the judicial authorities could order the intellectual property infringer to inform the identity of third persons involved in infringements.[25] In addition, the TRIPS Agreement includes some provisions that raise secrecy and confidentiality, but they look at commercial, business, and manufacturing information, not at personal information.[26]

ACTA calls attention to privacy and data protection in several of its drafted provisions by: drafting a provision to ensure that nothing in it detracts from domestic legislation regarding protection of personal privacy;[27] reserving domestic law that regulates processing of personal data, in accessing or disclosing personal information in civil enforcement[28] and

---

22 *Id.* art. 2.18.

23 The World Intellectual Property Organization adopted both the Performances and Phonograms Treaty and the Copyright Treaty, also known as the WIPO Internet Treaties, which provide protection for works in digital environment and regulates the technological protective measures, on December 20, 1996.

24 Adopted in 1998, the DMCA amended the U.S. Copyright Act, Title 17 of the U.S. Code, to comply with the WIPO Internet Treaties. However, beyond the purpose of the mentioned treaties, it also included provisions related to limitations on the liability of online service providers for copyright infringement. *See,* Digital Millennium Copyright Act, Pub. L. No. 105-304, 112 Stat. 2860, codified in scattered sections of 17 U.S.C. [hereinafter DMCA].

25 Agreement on Trade-Related Aspects of Intellectual Property Rights, Apr. 15, 1994, 1869 U.N.T.S. 299, 33 I.L.M. 1197 (1994) [hereinafter *TRIPS Agreement*], art. 47.

26 *Id.* arts. 34 and 39 (referring to secret information). *See also id.* arts. 40, 42, 43, 57 and 63 (referring to confidential information).

27 ACTA Draft – July 1, 2010, *supra* note 8, art. 1.4.

28 *Id.* art. 2.4.

border measures;[29] implicitly referring to the rights of defendants and third parties in enforcement;[30] excluding the monitoring of user monitoring by ISPs as a condition to enjoy the limitations on liability relating to material online;[31] requiring ISPs to provide expeditious information on the identity of subscribers to right holders in claims of copyright or related rights infringement;[32] and adopting privacy as a possible limit to transparency and/or publication of enforcement procedures and practices.[33]

As the Executive Director of the Electronic Privacy Information Center, Marc Rotenberg, correctly states, intellectual property rights never have conferred *per se* the right to identify users.[34] However, because enforcing intellectual property rights, particularly in the digital environment, requires identifying supposed infringers, ACTA has been forced to include the aforementioned provisions about privacy and personal data protection. They seem intended to balance the competing interests: reaching an appropriate level of enforcement for intellectual property and, at the same time, guaranteeing an adequate level of protection for privacy and personal data. Unlike intellectual property rights, which are "*private rights*,"[35] getting adequate protection for the rights to privacy and personal data is important not just for individual interests, but also to protect societal values, because they are essential in the very idea of democracy and as safeguards of human rights.[36]

In the following pages, this paper briefly analyzes the main challenges that the current text of ACTA creates for privacy and data protection, nascent provisions for an international treaty about intellectual property. This paper focus mostly on the context of intellectual property enforcement in the digital environment, but its conclusions may be applied generally to online and offline activities.

III. CRITICISMS OF ACTA'S PRIVACY PROVISIONS

---

29 *Id.* art. 2.13.
30 *Id.* art. 2.X.
31 *Id.* art. 2.18.3 *bis.*
32 *Id.* art. 2.18.3 *ter.*
33 *Id.* art. 4.3.
34 *The WIPO Copyright Treaties Implementation Act and Privacy Issues: Hearing on H.R. 2281Before the Subcomm. on Telecommunications, Trade, and Consumer Protection of the H. Comm. on Int'l Relations* (Jun. 5, 1998) (testimony and statement of Marc Rotenberg, Director, Electronic Privacy Information Center).
35 TRIPS Agreement, s*upra* note 25, Preamble.
36 *See* Frances S. Grodzinsky & Herman T. Tavali, *P2P Networks and the Verizon v. RIAA Case: Implications for Personal Privacy and Intellectual Property*, 7 ETHICS AND INFORMATION TECHNOLOGY 243 (2005).

Analyzing the current text of ACTA poses some challenges. First, most of the consolidated text is still in brackets, which means it is under discussion and there is not an agreement yet. Second, several provisions present different proposed options, some of them with important dissimilarities. Third, while some footnotes clearly evidence the negotiators' intent,[37] others seem an authoritative interpretation of the text,[38] still others look like they are primarily intended to reserve the agreement's implementation to the domestic law,[39] and even a few of them are directly prescriptive.[40] Those facts make it complex to identify the real intent of the negotiating parties and, therefore, how much of the current draft will be eventually in the agreement. However, in spite of those difficulties, it is still possible to attempt an analysis of the provisions of ACTA still under negotiation.

Probably because the EU has the strongest legal framework for protecting the rights to privacy and personal data protection, its authorities have reacted to and criticized the ACTA provisions for failing to provide adequate protection to those rights. Analyzing, and even describing, the legal framework to protect privacy and personal data adopted by the EU is beyond the purpose of this paper. Briefly, it provides a comprehensive legal regime for processing personal data related to physical persons, by automatic or manual process, for the public and private sectors. In the communitarian level, this framework includes specific provisions in the Charter of Human Rights[41] and several directives, such as the Data Protection Directive,[42] the Directive on Privacy and Electronic Communications,[43] and the Data Retention Directive.[44] As a general

---

37 *See, e.g.*, ACTA Draft – July 1, 2010, *supra* note 8, art. 2.18, and nn. 44, 47, 51, 59, and 61, (reserving the right to revisit elements of the draft later, but during the negotiations).

38 *See, e.g.*, *id.* art. 2.18 nn, 46, 50, 52, and 53. *See also id.* nn. 48 and 60 (defining terms).

39 *See, e.g.*, *id* art. 2.18 and nn. 43, 49, 54, 57, and 58.

40 *See, e.g.*, *id* art. 2.18 and nn. 55 and 56.

41 Charter of Fundamental Rights of the European Union, arts. 7 and 8, 2000 O.J (C 364) 10.

42 Council Directive 95/46, 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 the Free Movement of Such Data, 1995 O.J. (L 281) 31 [hereinafter Data Protection Directive].

43 Directive 2002/58, of the European Parliament and of the Council of 12 July 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector, 2002 O.J. (L 201) 37.

44 Directive 2006/24, of the European Parliament and of the Council of 15 March 2006 on the Retention of Data Generated or Processed in Connection with the Provision of Publicly Available Electronic Communications Services or of Public Communications Networks and Amending Directive 2002/58/EC, 2006 O.J. (L 105)

principle, the processing of personal data requires the express consent of the data subject, except for specific circumstances provided by domestic law, and independent national authorities guarantee the enforcement of the law.

In February 2010, one month after a version of ACTA was leaked, the European Data Protection Supervisor issued an opinion expressing his concerns about potential incompatibility between envisaged ACTA measures and the requirements of the EU's data protection law.[45] The Supervisor drew special attention to the provision dealing with the three strikes policy and the transfer of personal data to third countries, other than EU members, for purposes of intellectual property enforcement. Later, in July 2010, the Data Protection Working Party (WP29), which meets the national authorities on the matter, sent a public letter to the European Commission.[46] In its letter, the WP29 called attention to several of the proposed measures of ACTA interfering with the right to privacy, and called them into question for future negotiations. We will refer to the concerns of the EU authorities through our analysis.

The following pages describe the provisions of ACTA related with privacy and personal data, show how they connect with intellectual property enforcement, and analyze how they challenge the legal regime in force in countries that already have provided some protection to privacy and personal data, particularly those that are involved in the ongoing negotiations of the agreement.

A. ACTA Makes a Serious and Unprecedented Concession of Privacy and Data Protection in favor of Intellectual Property Enforcement

As was mentioned, ACTA makes several direct and indirect references to privacy and data protection, which are intended to balance them with intellectual property enforcement, unlike other major international instruments on intellectual property, which practically contain no mention of privacy and data protection. The very mention of them could be understood as an achievement for privacy advocates, because ACTA at least recognizes the importance of privacy and data protection by adopting specific norms that regulate its possible conflict with enforcing the

54 [hereinafter Data Retention Directive].

45 *Opinions of the European Data Protection Supervisor on the Current Negotiations by the European Union of an Anti-Counterfeiting Trade Agreement*, 2010 O.J. (C 147) 1.

46 Letter from the Article 29 Data Protection Working Party to the Commissioner, Mr. Karel de Gucht, regarding the Data Protection and Privacy Implications of the Anti-Counterfeiting Trade Agreement [ACTA] (July 15, 2010), *available at* http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/others/2010_07_15_letter_wp_commissioner_de_gucht_acta_en.pdf.

intellectual property law. However, in comparing ACTA with the TRIPS Agreement, those references seem to be a mere concession in favor of the enforcement.

In effect, the TRIPS Agreements recognize not only the relevant international intellectual property agreements or conventions, but also the applicability of the basic principles of the General Agreement on Tariffs and Trade (GATT) 1994 and, therefore, the General Agreement on Trade in Services, the multilateral treaties that set forth rules governing international trade in services, which the World Trade Organization (WTO) enforces. The latter includes a specific provision about general exceptions that allows countries to adopt of measures inconsistent with the Agreement when those measures are necessary to secure compliance with laws or regulations related to the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts.[47]

The mentioned general exception allows countries to develop public policies on several issues, without practical limitations, in fields such as safety, protection of the environment, public morals, to maintain public order, and personal data protection.[48] ACTA, on the contrary, requires countries to adopt given measures against the privacy and personal data protection of the Internet users in order to enforce intellectual property laws. In other words, while previous regulations safeguard the adoption of measures to protect privacy and personal data by countries, the ACTA provisions require the implementation of measures that negatively affect that privacy and personal data protection.

According to a still draft provision of ACTA, nothing in the agreement "shall require any party to disclose confidential information which would be contrary to . . . right of privacy."[49] This provision seems to safeguard the freedom of countries to provide an adequate level of protection for privacy and data protection. However, the scope of this safeguard is not clear yet; some countries wish to limit its effects to chapters about international cooperation and enforcement practices, but not the chapter that creates a

---

47 General Agreement on Tariffs and Trade (GATT 1947), art. XX; and, General Agreement on Trade in Services (GATS), art. XIV c) (ii).

48 *See* PETER SWIRE & ROBERT LITAN, NONE OF YOUR BUSINESS: WORLD DATA FLOWS, ELECTRONIC COMMERCE, AND THE EUROPEAN PRIVACY DIRECTIVE 191 (1998) (explaining limitations to the exception, none of them referred to intellectual property enforcement). In fact, it abides by several tests set forth by Article XIV of the GATS in order to prevent an abuse of the exceptions. *See* Council for Trade in Services, Work Programme on Electronic Commerce, Progress Report to the General Council, WTO document S/L/74 ¶ 14 (Jul. 27, 1999).

49 ACTA Draft – July 1, 2010, *supra* note 8, art. 4.3.2.

legal framework for enforcing intellectual property rights, which contains the riskiest provisions to privacy and personal data. In addition, this provision protects privacy, but only under determined circumstances.[50] As a result of those limitations, the mentioned safeguard does not prevent abuse in intellectual property enforcement or jeopardizing privacy and personal data protection.

Only by the ninth round of negotiations, among the initial provisions, was a second relevant safeguard proposed.[51] It also would allow parties to not disclose information related to privacy when that disclosure is "contrary to its law or its international agreements [and it] would prejudice law enforcement . . . or otherwise be contrary to public interest."[52] But, this safeguard, which is still under consideration,[53] has a broader scope than the aforementioned, and seems more satisfactory for the purpose of preserving and developing public policies consistent with the right to privacy in domestic laws, especially in those countries that understand privacy and data protection as issues of public interest, beyond the mere protection of the person concerned by the information.

In sum, ACTA has made a serious and unprecedented concession of privacy and data protection in favor of intellectual property enforcement by depriving countries of the freedom to adopt laws related to protecting the rights to privacy and personal data protection, and by requiring the implementation of measures that negatively could affect those rights. In other words, ACTA does not prevent the adoption of public policies on privacy and data protection by countries, but certainly imposes some conditions on them. Including a general safeguard in ACTA would help to preserve and develop some adequate protection in domestic law; however, it does not change that significant concession.

B. ACTA Still Omits Appropriate Safeguards for the Right to Privacy in General.

As previously discussed, the current text of ACTA does not include any

---

50 *Id.* art. 4.3.2 (drafting a proposal that sets forth parties will be not required to disclose information which would *"impede the enforcement"* of its laws and regulations, including laws protecting the right to privacy. Therefore, any other case, parties shall be required to).

51 *See id*. (expressing interest in including a general safeguard in favor of the right to privacy by the 8th round of negotiation, which seems quite late, given the importance of this right, particularly for the European Union).

52 *Id.* art. 1.4.

53 *Id.* n. 3 (mentioning that this provision is still subject to confirmation by the United States and the New Zealand delegations).

general provision that ensures that nothing in the agreement detracts from domestic legislation regarding the protection of personal privacy. However, as was mentioned, there is a proposal to include a provision with that purpose,[54] which unfortunately has not been confirmed by some negotiators yet.[55] This norm is essential, given the concession that ACTA has made with privacy and data protection in favor of intellectual property enforcement and the absence of appropriated limitations and safeguards in other international instruments in both data protection and intellectual property regulation.

It is possible to argue that other international instruments on human rights already protect the right to privacy and the right to personal data protection against a possible abusive enforcement of intellectual property laws, but, unfortunately, those instruments have limited effects. Some of them have limited personal effects, such as the Charter of Fundamental Rights of the European Union.[56] Most of them are not legally binding[57] and, therefore, almost impossible to enforce.[58] Others could be legally binding but have an extremely generic and ambiguous enunciation of those rights.[59] In some countries, like in the U.S., human rights in general have a limited enforcement against the public sector, but not the private one.[60]

In sum, the international instruments on human rights still are insufficient to provide adequate protection for the right to privacy and for the right to protection of personal data against the threat posed by the level of intellectual property enforcement encouraged by ACTA. In addition, no

---

54 *Id.* art. 1.4.

55 *Id*.

56 *See* Data Protection Directive, *supra* note 42.

57 *See Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, OECD Council (Sept. 23, 1980). *See also* United Nations Guidelines Concerning Computerized Personal Data Files, G.A. Res. 45/95, U.N. Doc. A/RES/45/95 (Dec. 14, 1990); Asia-Pacific Economic Cooperation Privacy Framework, APEC XVI Ministerial Meeting, November 17-18, 2004, *available at* http://www.ag.gov.au/www/agd/rwpattach.nsf/VAP/%2803995EABC73F94816C2AF4AA2645824B%29~APEC+Privacy+Framework.pdf/$file/APEC+Privacy+Framework.pdf.

58 These instruments would only be enforceable if they become customary norms, which seems difficult because they have been intended as a non-binding rules and mere recommendation for parties, denying *opinio juris*, an essential element for customary law.

59 *See* Universal Declaration of Human Rights, G.A. Res. 217 (III) A, U.N. Doc. A/RES/217(III) (Dec. 10, 1948); U.N. Charter (Jun. 26, 1945).

60 For a limited number of cases in which the U.S. accepts enforcement of human rights against the private sector, *see, e.g.*, The 1789 Alien Tort Claims Act, 28 U.S.C. §1350 (1988); Filartiga v. Peña-Irala, 630 F.2d 876 (2d Cir. 1980); and, the Torture Victim Protection Act of 1991, 28 U.S.C. § 1350, Pub. L. 102-256, 106 Stat. 73 (codifying

international instrument in either data protection or intellectual property currently provides safeguards to reconcile the competing interests. For those reasons, it seems indispensable to include, in the very text of ACTA, a general provision to ensure that nothing in the agreement detracts from domestic legislation regarding the protection of personal privacy.

C. ACTA Grants Access to Internet Users' Personal Information for Intellectual Property Enforcement beyond Domestic Laws in Force

Enforcing the law in the digital environment to address individual infringement requires the identification of infringers and, consequently, the collaboration of the online service providers (OSP) with the right holders. OSPs have been collecting and processing Internet users' personal data for a long time, initially for pricing purposes,[61] later by law in order to contribute to criminal prosecution, especially with regard to so-called cyber crime.[62] Knowing the IP address,[63] and the date and time of connection, OSPs are able to identify the connected computer. Once knowing the connected computer, it is possible to correlate it with the Internet user's identity and his physical address.[64]

Several provisions of ACTA persist in granting access to information that allows identifying supposed intellectual property infringers: in relation to civil enforcement in general,[65] to border measures,[66] and in enforcing the

---

Filartiga).

61 Before offering Internet service access on a flat rate basis, companies used a price structure based in the amount of time of connection, a metered rate that depended on processing some Internet users' personal data for pricing purposes.

62 *See* Convention on Cybercrime, Budapest 23.XI.2001 (ETS No. 185) (Nov. 23, 2001), *available at* http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm [hereinafter Convention on Cybercrime]; Susan W. Brenner, *The Council of Europe's Convention on Cybercrime*, *in* CYBERCRIME: DIGITAL COPS IN A NETWORKED ENVIRONMENT 207 (Balkin ed., 2007) (arguing that country parties of the Convention have been unable to adopt even a common understanding on criminal prosecution; in fact, the agreement is not self-executing, does not provide a model legislation, allows reservation by parties, and fails to provide an adequate understanding of the privacy rules on the matter).

63 An IP address is a number assigned to any device (computer) connected to the Internet. Sometimes that number varies according to the time of connection and is assigned on demand by the Internet service provider (dynamic IP address); in other instances that number is permanently linked to a given device (permanent IP addresses).

64 This tracking system allows the identification of computers rather than users. In fact, in some cases it is necessary to adopt additional technical measures to identify a user, such as in open network (e.g., universities use a user name and password, while cybercafés use a register identifying users).

65 ACTA Draft – July 1, 2010, *supra* note 8, art. 2.4 (including a still in bracket provisions by the eighth round, which makes reservation in favor of domestic laws

law in digital environment.[67] However, while in the first two cases, negotiators have approved the inclusion of express safeguards related to statutory provisions that regulate the processing of personal data and privacy laws, that did not happen in the third case;[68] instead, in this case, a proposal emphasizes that parties shall enable right holders to "expeditiously" obtain from OSPs the necessary information to identity the subscriber that supposedly has infringed the law.[69]

Many countries already have laws that allow the copyright holder to access such information from OSPs.[70] However, the current text of ACTA goes beyond any domestic law by adopting an extremely broad concept of online service provider; by extending the scope of those provisions; and by omitting mention of any safeguards.

The obligation to identify subscribers applies to any online service provider, which is defined by the same ACTA provision in the following terms:

> a provider of online services or network access, or the operators of facilities therefore, and includes an entity offering the transmission, routing, or providing of connections for digital online communications, between or among points specified by a user, of material of the user's choosing, without modification to the content of the material as sent or received.[71]

This definition is broader than those available in comparative law, since it applies to any person, including physical persons, to any provider, even those that only provide access, and, not only to Internet based providers, but any online service.

---

that regulate processing of personal data).

66 *Id.* art. 2.13 (including an already approved reservation in favor of laws pertaining to the privacy or confidentiality of information).

67 *Id.* art. 2.18.3 *ter*.

68 *See id*. According to the first leaked version, those safeguards, which appear approved by the second leaked version, were promoted by the European Union and Singapore, respectively.

69 *See id*.

70 This is not the case of all the countries involved in the ACTA negotiations. In fact, Mexico does not have legal provisions related to liability of online service providers for copyright infringement, neither notice-and-takedown procedures nor rules related to identifying subscribers by online service providers for supposed copyright infringement.

71 It seems parties agree on the definition of online service provider, since, with the exception of a mere cosmetic Canadian proposal, no other proposal has been raised, and there is no record of opposition by any other country in any version of the agreement. *See, e.g.*, ACTA Draft – July 1, 2010, *supra* note 8, n. 48.

In the U.S., procedures for taking down content and identifying users are limited to a service provider that is an "entity,"[72] that is, "an organization (such as a business or a governmental unit) that has a legal identity apart from its members."[73] In other words, those procedures apply only to legal persons, but not to physical persons or human beings. Instead, according to ACTA, those provisions shall apply to any provider, which "*includes an* entity." Therefore, at least in the case of the U.S. and countries that have adopted similar provisions to the DMCA in their FTAs,[74] ACTA extends the duties, obligations, and cost of intellectual property enforcement not just to legal persons, but possibly to common people.

In the U.S., according to the criterion of the *Verizon* case,[75] the procedures to identify subscribers set forth by the DMCA do not grant access to information that allows identification of users by a mere access provider.[76] In the EU, the E-Commerce Directive, which regulates the procedure to identify users, does not include mere providers of access, but those that provide storage services.[77] Instead, ACTA would extend the obligation to identify users to firms that only provide access to networks in their capacity as conduit because ACTA does not make any distinction

---

72 17 U.S.C. § 512(k) (2006).

73 BLACK'S LAW DICTIONARY (9th ed. 2009).

74 The U.S. has included similar provisions in the Free Trade Agreements successively signed with Singapore, Chile, Morocco, Australia, Costa Rica, El Salvador, Guatemala, Honduras, Nicaragua and Dominican Republic, Bahrain, Oman, Peru, Colombia, and Panama. *See* United States Trade Representative, http://www.ustr.gov/trade-agreements/free-trade-agreements.

75 RIAA v. Verizon Internet Services, Inc., 351 F.3d 1229, 1237 (D.C. Cir. 2003).

76 Commentators agree that the Verizon case has been a triumph for privacy advocates, but it has not seriously affected the copyright holders' policies because they still can issue subpoenas, which are available to any litigant who wants to sue an unknown defendant by filing against *John Doe*. This mechanism provides more substantive and procedural protection for Internet users, but it is not enough to avoid misuse and abuse of the procedure. As a result, according those commentators, even in the case of OSPs that provide mere access, copyright owners still have legal tools against infringers in the civil enforcement context. *See* Alice Kao, *RIAA v. Verizon: Applying the Subpoena Provision of the DMCA*, 19 BERKELEY TECH. L.J. 405, 418, 422-426 (2004); Thomas P. Owen & A. Benjamin Katz, *RIAA v. Verizon Internet Services, Inc.: Peer-to-Peer Networking Renders Section 512(h) Subpoenas under the Digital Millennium Copyright Act Obsolete*, 24 LOY. L.A. ENT. L. REV. 619, 632-634 (2004).

77 Directive 2000/31 of the European Parliament and of the Council of 8 June 2000 on Certain Legal Aspects of Information Society Services, in particular Electronic Commerce, in the Internal Market, art. 15.2, 2000 O.J. (L.178) 1. *But see* Case C-557-07, *Oberster Gerichtshof (Austria) - LSG-Gesellschaft zur Wahrnehmung von Leistungsschutzrechte GmbH v Tele2 Telecommunication GmbH* (Feb. 19, 2009) (deciding, in spite of the literal wording of the mentioned Directive, that the obligation to identify users could be imposed on access providers, even when they do no supply any other service).

related to this obligation,[78] as opposed to the notice-and-take-down procedure,[79] and to the kind of service provided by OSPs.[80] Therefore, the implementation of this obligation could require a modification to the DMCA under U.S. law,[81] domestic laws drafted according FTAs,[82] and the EU Directive on E-Commerce.

The definition of online service provider not only applies to any person and provider, even those that only provide access, but also to any online service, not only Internet based providers. Instead, the EU law limits the collection of personal data generated or processed by "providers of publicly available electronic communications services or of a public communications network."[83] Therefore, ACTA could undermine this standard, by applying the obligations to online service providers that are not yet addressed in the current EU law, such as private network services.[84]

The obligation to identify subscribers set forth by ACTA has a broad scope also. They seem not limited to copyright enforcement, but intellectual property; additionally, they extend not only to piracy and counterfeiting, as it was suggested by negotiating parties, but, also, to criminal and civil enforcement of intellectual property rights in general.

By the ninth round of negotiations, it is still unclear whether the obligation to identify subscribers applies only to copyright and related rights or also to other intellectual property rights. While the specific provision related to enforcement in the digital environment seems to limit the scope to trademarks, copyright, and related rights,[85] the whole section refers to intellectual property rights, and some countries seem to be pushing for such a broad approach.[86] The latter could be especially problematic for

---

78 ACTA Draft – July 1, 2010, *supra* note 8, arts. 2.18.3 *ter* and 2.18.3 *quarter*, and n. 48.

79 *Id*. art. 2.18.3. *See also,* ACTA Draft – Jan. 18, 2010, *supra* note 8 art. 2.18.3 (excluding from the notice and take down procedures those providers acting solely as a conduit).

80 *See supra* note 71.

81 17 U.S.C. § 512 (2006).

82 This could be the case of Chile, which in May 2010 implemented the FTA signed with the U.S., imposing the obligation to identify users on ISPs other than those that provide mere access. *See* Ley 17.336 sobre Propiedad Intelectual, [Copyright Act], *as amended,* Diario Oficial, 4 de Mayo de 2010 (Chile), arts. 5 y, 85 R, and 85 S.

83 Data Retention Directive, *supra* note 44, art. 3.

84 Curiously, it is possible to appreciate a disagreement between those countries that want to apply this section to "*the Internet*" (Mexico, Singapore, and the United States) and those that want to extend the scope to "*digital environment*" (the European Union and Switzerland), which are already the words in the provisional title of the whole section. *See* ACTA Draft – July 1, 2010, supra note 8, art. 2.18.1.

85 *Id.* art. 2.18.3 *ter*.

86 Australia, Canada, Mexico, New Zealand, Singapore, and the United States support a scope limited to trademark, copyright and related rights, while the European Union,

the U.S., since the DMCA limits its provisions to enforce copyright and related rights; therefore, a full compliance with that scope of the ACTA provisions would force the adoption of legislative measures.

In addition to the fact that the scope of the obligation to identify subscribers is still unclear, it is important to point out that they do not apply only to serious crime, either counterfeit or piracy, but to any criminal behavior. Going beyond its declared purposes, ACTA requires identifying any infringer, even when the conduct is neither counterfeiting nor piracy. Although ACTA recognizes some gradation among criminal conduct,[87] for purpose of identifying users, the agreement does not make any distinction and seems to apply to any criminal activity. Given the initial purpose of the agreement and the lack of consensus about what constitutes a criminal offense,[88] it seems necessary to introduce some gradation in the cases that authorize OSPs to identify users by limiting that procedure to criminal actions concerning counterfeiting and piracy.[89]

The obligation to identify subscribers in ACTA applies not only in criminal enforcement, but also in civil enforcement.[90] Neither the provisions that grant access to subscriber information, nor those related to the civil enforcement section of the agreement, which also apply to enforcing the law in the digital environment,[91] exclude the obligation to identify Internet users from civil enforcement. This is a troublesome scope, since most countries requires OSPs to retain traffic data for purposes of criminal prosecution, especially in the cases of so-called cyber crime,[92] but such obligation does not apply to civil enforcement actions. The underlying belief is that granting access to personal data of Internet users processed by OSPs jeopardizes human rights and the essential values of a democratic society, a risk that cannot be tolerated for mere civil enforcement of

---

Japan, and Switzerland a broader approach, which extends to all intellectual property rights. *Id.* art. 2.18.1.

87 *E.g., id.* arts. 2.14.1 (referring to criminal offenses in "*cases of willful trademark counterfeiting or copyright or related rights piracy on a commercial scale*"), 2.16.3 (mentioning "*indictable offenses*" and "*serious offenses*"), and 2.17 (referring to "*cases of significant public interest*"). *Also, see id.* art. 2.X (providing an exception to border measures in case of *di minimis* infringement, which is not the case for granting access to personal data related to a supposed infringer).

88 *Id.* art. 2.14.1.

89 *Id.* nn. 20, 21, 23 and 24 (providing concepts for both counterfeit trademark goods and pirated copyright goods, which, however, are considerable broad and require some changes in order to rationalize the scope of the criminal enforcement provisions yet).

90 *Id.* art. 2.18.1.

91 *Id.* art. 2.4.

92 *See* Convention on Cybercrime, *supra* note 62, art. 14.

intellectual property rights that, after all, according to the TRIPS Agreement, are private rights.[93]

In the case of the EU, for example, the Data Retention Directive requires providers to process subscribers' personal data for purpose of the investigation, detection, and prosecution of serious crime.[94] However, according to the decision of European Court of Justice in the *Promusicae* case.[95] Community law does not set forth a specific obligation upon EU members to guarantee access to Internet users' personal data to copyright holder in civil enforcement actions, but Community law does allow the adoption of this kind of measure in the domestic law.[96] In sum, for the EU, although it would be permitted by Community law, ACTA would require adopting a law that obliges providers to identify subscribers for purposes of civil enforcement.[97]

In sum, ACTA would grant access to the personal information of subscribers held by providers for intellectual property enforcement beyond the domestic laws in force. According to the initial purposes of ACTA, it is recommended to expressly limit the scope of such access to information, for example, by limiting that access to cases of criminal actions in counterfeit and piracy and, therefore, excluding civil enforcement actions.

D. ACTA omits appropriate safeguards for the right to personal data protection in providing access to personal information of Internet users.

As was previously mentioned, ACTA grants access to Internet users' personal information for purposes of intellectual property enforcement. However, ACTA fails to provide enough measures to protect the rights of concerned people from an abusive use of that access mechanism. On the contrary, ACTA seems to privilege expeditious access to data, without

---

93 *See supra* note 35.

94 Data Retention Directive, *supra* note 44, art. 1.

95 ECJ Case C-275/06, *Productores de Música de España (Promusicae) v. Telefónica de España SAU* (Jan. 29, 2008).

96 *Contra* Ramón Casas Vallés, *A la Caza del Pirata P2P: El Necesario Equilibrio entre el Derecho de Autor y el Derecho a la Protección de la Intimidad*, WIPO MAGAZINE (Spanish version), April 2008, at 10-11 (suggesting that the message of ECJ is that the EU members are not required to impose such kind of obligation in civil procedures, but it is recommended). *But see*, Ramón Casas Vallés, *Pursuing the P2P Pirates: Balancing Copyright and Privacy Rights*, WIPO MAGAZINE (English version), April 2008, at 10-11 (providing a right understanding of the implications of Promusicae case).

97 *See also supra* note 46 (calling the attention of the WP29 about the different scope of the ACTA provisions and the European Union law).

mentioning either substantive or procedural safeguards.[98]

Negotiators recently have included an article in ACTA that safeguards domestic privacy laws. However, that general statement is insufficient to protect privacy and personal data processing properly in the context of intellectual property enforcement online. Specifically, ACTA fails to provide any provisions that set forth how much time OSPs should keep subscribers' personal data, procedures that properly guarantee the rights of concerned subscribers, or even which data should be kept.[99] It also has been noted by the EU authorities[100] that ACTA does not adopt any temporal limitation for the processing of personal data by Internet service providers, which is another possible conflict with EU law.[101]

The absence of appropriate safeguards is contrary to the high standards of protection adopted by the EU, and even the minimal formal requirements provided by the DMCA in the U.S. In the EU, according to the European Court of Justice, members that wish to implement into domestic law a mechanism to identify Internet users must balance fundamental rights, and national authorities must interpret their domestic laws in a manner consistent with fundamental rights, and with the other general principles of Community law, such as the principle of proportionality.[102] In the U.S., even the most expeditious procedure to identify a supposed infringer provided by the DMCA has some minimal required showings,[103] which basically require filing a couple of documents.[104] Even these minimal safeguards are absent in ACTA.

Added to the lack of harmonization between ACTA provisions and both the EU and the U.S. domestic laws, the absence of explicit safeguards in the agreement can become a serious problem in its own implementation, particularly for those countries lacking adequate technical assistance. It is a well-known fact that some countries implement their international commitments, especially with regard to technical issues, in a word-by-word legal fashion. For that reason, it is recommended to include some specific

---

98 ACTA Draft – July 1, 2010, *supra* note 8, art. 2.18. 3 *ter*.

99 Some of those safeguards (and useful boundaries) are usual in other instruments, particularly in the European Union law. *See, e.g.*, Data Retention Directive, *supra* note 44; *see also* Convention on Cybercrime, *supra* note 62.

100 *See supra* note 46.

101 Data Retention Directive, *supra* note 44, art. 6.

102 *See* ECJ Case C-275/06, *Productores de Música de España (Promusicae) v. Telefónica de España SAU* (Jan. 29, 2008).

103 *See* Julie E. Cohen et al., *Copyright & Privacy – Through the Privacy Lens*, 4 J. MARSHALL REV. INTELL. PROP. L. 273, 273 *et seq.* (2005) (arguing that the relevant DMCA's provisions are excessively permissive and threats seriously the privacy); *See also* Owen & Katz, *supra* note 76, at 620; and, Kao, *supra* note 76, at 410.

104 17 U.S.C. §512(h)(2) (2006).

provisions in ACTA that give a common level of protection for the rights to privacy and personal data. In this point, following the aforementioned criteria of the European Court of Justice seems to be the most appropriate decision.

E. ACTA Provides Legal Support for Implementing the Polemical Three Strikes Policy, a Measure that Raises Several Concerns from a Human Rights Perspective.

The three strikes policy, also known as the *graduated response*, is a measure of domestic law that allows the disconnection of a supposed infringing Internet user for a given period of time, after the user has received warning with successive notices about copyright infringements committed through his or her Internet account. At the time this paper was written, only a handful of countries had passed laws adopting three strikes provisions, including France,[105] South Korea,[106] Taiwan,[107] the United Kingdom,[108] and New Zealand.[109]

The French three strikes law was introduced by Sarkozy's government, and it is probably the most illustrative case about how polemical this policy can be. The bill generated serious concerns in the French data protection authority related to the protection of Internet users' personal data.[110] Later, once adopted by the legislature, the law was declared unconstitutional by the Constitutional Council[111] because it infringed the right to due process of law by allowing an administrative authority to impose sanctions,[112] by-

---

105 Bill to support the diffusion and protection of content on the Internet, also known as HADOPI Act, because the acronym of the Haute Autorité pour la Diffusion des Oeuvres et la Protection des droits sur Internet, the name of the administrative agency that supervises its compliance.

106 Art. 133 *bis*, South Korean Copyright Act, modified in April 2009.

107 Art. 90 *quinquies*, Taiwanese Copyright Act, modified in May 2009.

108 Digital Economy Act, 2010, c. 24 (Eng.).

109 The Copyright (New Technologies) Amendment Act, adopted in April 2008, modified the copyright law by adopting a three strikes provision, which was later modified by the Copyright (Infringing File Sharing) Amendment Bill, 2010.

110 Commission nationale de l'informatique et des libertés, Délibération no. 2008-101 du 29 avril 2008 portant avis sur le projet de loi relatif à la Haute Autorité pour la diffusion des œuvres et la protection des droits sur Internet (avis no. 08008030), published unofficially as La Loi Antipiratage: le Gouvernement Critiqué par la CNIL, published in La Tribune, 3 November 2008, *available at* http://www.latribune.fr/entreprises/communication/telecom--internet/20081103trib000305843/loi-antipiratage-le-gouvernement-critique-par-la-cnil-.html (last visited: August 30, 2010).

111 Conseil constitutionnel [CC] [Constitutional Council], decision no. 2009-580, Jun. 10, 2009.

112 *Id.* ¶ 16.

passing the presumption of innocence by requiring the subscriber to prove he or she has not committed an infringement,[113] and the right of free speech because "in the current state of affairs . . . the participation in democratic life and expression of ideas and opinions includes the freedom to access to those services (Internet)."[114] Eventually, the unconstitutionality was remedied by the French Parliament, which empowered courts to disconnect Internet users.[115] However, after one year in force, no one has been warned of infringement nor disconnected; as Jérémie Zimmermann, the spokesperson of La Quadrature du Net, a French advocacy group that promotes rights and freedoms on the Internet, said, the law has created a "big tax-sponsored spam machine."[116]

The French three strikes law also affected the communitarian level. In fact, Sarkozy's initiative created a conflict between the European Commission, then under the presidency of the French government, and the European Parliament in the context of the adoption of the Telecom Package. The conflict eventually was solved by adopting an amendment resisted by Sarkozy's government, which requires that "measures taken by countries regarding end-users' access . . . shall respect the fundamental rights and freedoms of natural persons, as guaranteed by the European Convention for the Protection of Human Rights and Fundamental Freedoms and general principles of community law."[117]

The leaked versions of ACTA included an explicit mention of the three strikes laws in footnotes, as an example of a policy to address the unauthorized storage or transmission of materials protected by copyright or related rights that could be adopted and reasonably implemented by OSPs in order to qualify for the limitation of liability related to online material.[118] The content of that footnote has been deleted in the official version of ACTA, but ACTA still keeps provisions to support the three strikes policy. Therefore, with or without explicit mention in footnotes, even when ACTA does not require the adoption of three strikes laws, it provides legal support for implementing this polemical measure.

---

113 *Id.* ¶ 17. Interestingly, this is a common feature of all the three strikes laws already adopted: the user is presumed guilty in advance and, therefore, she must probe being innocent, in spite of her technical limitations.

114 *Id.* ¶ 12.

115 Assemblée Nationale, Projet de Loi relatif à la protection pénale de la propriété littéraire et artistique sur Internet (Sept. 22, 2009).

116 *Hadopi is dead: "three strikes" buried by highest court*, La Quadrature (Paris), Jun. 10, 2009, http://www.laquadrature.net/fr/hadopi-is-dead-three-strikes-killed-by-highest-court.

117 Council Directive 2009/140, art. 1 (1) (b), 2009 O.J. (L 337) 37.

118 *See* ACTA Draft – Jan. 18, 2010, *supra* note 8, n. 29; *See also European Union Directorate-General For Trade, ACTA Negotiations* (Sept. 30, 2009), Ref. 588/09.

In addition to human rights concerns, disconnecting Internet users, as ACTA suggests, should be especially cumbersome for countries that already have recognized the rights to access to Internet and/or to broadband.[119] But it is not just the sanction of disconnection itself that causes concern, but also the lack of substantive and procedural safeguards for supposed infringers. For example, ACTA does not impose a general monitoring requirement on OSPs,[120] but the very implementation of a three strikes provision requires some processing of personal data without authorization of the data subject; again, ACTA fails in providing a minimum legal framework for such data processing. In this point, given that the appropriate operation of a three strikes policy requires identifying a supposed infringer, all the comments made previously are also valid here.

The European authorities on data protection have analyzed the ACTA provisions on three strikes and their negative effects on the right to privacy. According to the European Data Protection Supervisor and the WP29,[121] the current text of ACTA at the very least encourages the implementation of the controversial three strikes policy. They argued that the agreement should include some "minimum standards for the enforcement," and called to attention that large scale monitoring or systematic recording of data would be contrary to the EU law.

Any explicit reference to the three strikes policy should be avoid in ACTA because it could be used as a argument to force countries to implement such a polemical measure. Otherwise, given its intrinsic punitive nature, the three strikes policy should be brought into compliance with the basic principles of criminal and human rights law, such as *nullum poena sine legem* (principle of legality), *non bis in idem* (prohibition of double incrimination), the presumption of innocence, and the due process of law. Therefore, similar to what the French Constitutional Council and the Telecom Package have done,[122] a direct or indirect reference to such policy should be mitigated with express allusion to substantive and procedural safeguards with respect to the fundamental rights and freedoms of persons.

---

119 *See Finland makes broadband a 'legal right,'* BBC (London), Jul. 1, 2010, *available at* http://www.bbc.co.uk/news/10461048 (last visited: August 30, 2010) (reporting that Finland recently has become the first one to recognize access to the Internet as a legal right).

120 ACTA Draft – July 1, 2010, *supra* note 8, art. 2.18.3 bis.

121 *See supra* notes 45 & 46.

122 *See supra* notes 111 &117.

F. ACTA promotes cooperation between rights holders and ISPs without regard for the rights of third parties, like the right to privacy and protection of personal data of customers.

A still unapproved article of ACTA requires parties to promote the development of mutually supportive relationships between OSPs and rights holders to deal with intellectual property infringement online, including encouraging the establishment of guidelines.[123] In this context, promoting self-regulation seems an adequate manner to deal with the continuous changes and challenges of the technological environment, and with the usual delay of legal solutions. However, again ACTA fails in not providing any safeguards for the right of third parties, particularly the Internet end-users.

It is important to note here that the self-regulatory approach has been used in some countries, such as the United Kingdom[124] and Ireland,[125] to promote the adoption of three strikes policies by the OSPs. Under pressure from copyright holders and with the implicit agreement of governments, OSPs have modified their contracts with subscribers to include clauses that legitimate the disconnection of users for supposed copyright infringements. Unfortunately, this self-regulation has not protected customers' rights appropriately. ACTA should take advantage of these experiences and include safeguards against abusive self-regulatory practices.

G. ACTA Emphasizes the Protection of Effective Technological Measures, but Still Does Not Afford Protection for the Privacy and Personal Data of Users Affected by Such Measures.

The ACTA negotiators have provided a significant increase in the legal protection of the effective technological measures beyond the standard adopted in the WIPO Internet Treaties.[126] Before the public official release of ACTA, it required not only adequate legal protection and effective legal remedies, but also civil remedies or criminal penalties,[127] an excess that

---

123 ACTA Draft – July 1, 2010, *supra* note 8, art. 2.18.3 *quater*.

124 *See* Eleanor Dallaway, *Music Piracy Born Out of a 'Something for Nothing' Society*, INFOSECURITY 17-20 (Apr. 2008); Christian L. Castle & Amy E. Mitchell, *What's Wrong With ISP Music Licensing?*, 26 ENT. & SPORTS LAW. 4, 7 (2008).

125 Karlin Lillington, *Putting Up Barriers to a Free and Open Internet*, THE IRISH TIMES, April 16, 2010.

126 *See* World Intellectual Property Organization Copyright Treaty, Dec. 20, 1996, S. Treaty Doc. No. 105-17, 36 I.L.M. 65 (1997), art. 11; World Intellectual Property Organization Performances and Phonograms Treaty, Dec. 20, 1996, S. Treaty Doc. No. 105-17, 36 I.L.M. 76 (1997), art. 18.

127 ACTA Draft – Jan. 18, 2010, *supra* note 8, art. 2.18.4.

does not appear in the current draft of ACTA. But, ACTA still requires the adoption of those remedies independent of any infringement of copyright or related rights.[128] Also, similar to the DMCA,[129] ACTA still requires adopting anti-circumventing and anti-trafficking provisions,[130] the latter of which implies serious difficulties in making real the possible safeguards that a country "may" adopt in benefits of certain exceptions and limitations to copyright and related rights.[131] Unfortunately, unlike the DMCA and the FTAs signed by the U.S. with several countries, ACTA does not provide even a minimum list of those exceptions.

Analyzing the provisions about legal protection of the effective technological measures is beyond the purpose of this paper. However, it is appropriate to mention that those provisions again fail in including any limitation that guarantees the adequate protection of the rights to privacy and personal data protection. Including a provision that provides safeguards for those rights is necessary insofar as the technological measures require personal data of people who use or access to the protected works.

H. ACTA omits provisions to safeguard the protection of personal data in cross-border transferences of such data.

The whole purpose of getting compliance with intellectual property rules and enforcing them requires, to some extent, interchanging personal information among parties, such as copyright holder and supposed infringers' data. This is especially true in the case of online infringements; overcoming the limitations of territorial-based domestic laws demands a global answer, which calls for international cooperation in the enforcement of the law. In the case of ACTA, it sets forth that countries that adhere to the agreement shall share relevant information[132] and adopt some enforcement practices.[133] Unfortunately, there is no provision that safeguards that an adequate level of protection shall be provided to the personal data that is transferred from one country to another. In other words, ACTA forgets the existence of rules that regulate the cross-border transference of personal data.

Several countries already have personal data protection laws, which

---

128 ACTA Draft – Jul. 1, 2010, *supra* note 8, art. 2.18.5.

129 *See* 17 U.S.C. § 1201(1)(A) (2006) (including anti-circumvention provisions); 17 U.S.C. §1201(a)(2) (2006) (including anti-trafficking provisions).

130 ACTA Draft – Jul 1, 2010, *supra* note 8, art. 2.18.4.

131 *Id.* art. 2.18 X.

132 *Id.* art. 3.2.

133 *Id.* Ch. 4 Enforcement Practices.

balance the protection of people's privacy with the free flow of information. However, as it was understood early on by the European countries, the very purpose of having strong domestic protection could be eroded if personal data is transferred to countries with no protection; cross-border transferences of personal data to places where there is not an adequate level of protection circumvents the objective of data privacy laws. Therefore, it is necessary to adopt some limitations to those transfers, which unfortunately ACTA does not do.

It is not by chance that the European Data Protection Supervisor has raised the lack of provisions on cross-border transfers of personal data in ACTA.[134] There have been some attempts to regulate those transfers in international *fora* through legal harmonization, but their successes, if they exist, have been limited.[135] But, this has not been the case of the EU. Since the early '80s,[136] the EU has built an increasing level of protection for personal data in its internal market, which has been catapulted through the adoption of several directives on the matter.[137] Basically, this legal framework assumes an "*equivalent*" level of protection among the EU members, which cannot block transfers in the internal market;[138] and, requires an "*adequate*" level of protection to third countries in order to authorize transfers of data to them.[139] Therefore, apart from some limited exceptions,[140] transferring personal data to third countries that do not provide adequate level of protection, which is the case of all the countries involved in the ACTA negotiations, is banned.

It seems that the ACTA negotiators have avoided acknowledging the fact that a satisfactory solution for transferences of personal data is required for intellectual property enforcement in the agreement. This is hardly a small point, especially for the European authorities that are more concerned with the protection of European citizens, and particularly their right to privacy. In fact, two of the main political conflicts between the European Parliament and the European Commission, which is negotiating ACTA, have been the result of the most sympathetic engagement of the former than the latter in protecting the right to privacy: first, when the Parliament

---

134 *See supra* note 45.
135 *See supra* note 57.
136 *See* Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, January 28, 1981 (attempting for first time the harmonization of personal data protection law among countries; in this case, countries of the European community).
137 *See supra* notes 42, 43, and 44.
138 Data Protection Directive, *supra* note 42, at 8, 9.
139 *Id.* at 56, 57, 59, 60; and art. 25.
140 *Id.* art. 26.

rejected the agreement between the Commission and the U.S. to transfer personal data of air passengers; later, when the Parliament adopted a provision against the three strike policy in the Telecom Package against the Commission's desires. These facts show that privacy is a serious issue for European authorities, which ACTA negotiators have not weighed properly.

IV. CONCLUSIONS AND REMARKS

Authorizing any intrusion into the privacy and personal data protection of Internet users under the guise of intellectual property enforcement is disproportionate, and allows an excessive misuse and abuse of disclosed information, which jeopardizes not just the right to privacy, but also an essential requirement for a democratic society. But, at the same time, denying access to information that is required to identify an infringer, particularly the author of a serious infringement, is excessive. ACTA has had to balance the competing interests in this dilemma: the rights to privacy and the protection of personal data with intellectual property rights.

The concessions of ACTA in privacy exceed the very purpose of the treaty, which pretends to be limited to fighting counterfeiting and piracy, but instead it includes provisions intended to enforce the law against citizens. Those serious and unprecedented concessions omit appropriate substantive and procedural safeguards for the right to privacy of Internet users. Instead of limiting the access to personal data to serious crimes, ACTA grants access to personal information beyond domestic laws in force. Even other international instruments that have been criticized seriously for being intrusive on privacy, such as the Convention on Cybercrime and the FTAs, seem more protective on the matter.

In addition, ACTA provides legal support for implementing the polemical three strikes policy, a measure that raises several concerns from a human rights perspective, and promotes cooperation between right holders and ISPs without regard to the rights of third parties, such as the right to privacy and protection of personal data of customers. The same can be said about the provisions related to the protection of effective technological measures, which do not afford any protection for the privacy and personal data of users affected by them.

An additional serious problem arises in the harmonization of the provisions of ACTA, which implicitly allow transferences of personal information among the parties, and the EU requirements for trans-border flow of personal data. Currently, none of the negotiating parties satisfy the EU "*adequate*" level of protection to allow transferences of personal data; therefore, national and communitarian authorities on data protection in the

EU could block any transference of such data for intellectual property enforcement. And, even worse for the intentions of negotiators, it can become an obstacle for the adoption of ACTA by the European Parliament.

ACTA fails not only in providing adequate protection for the rights to privacy and the protection of personal data, but also in addressing its very purpose, in providing a harmonizing international instrument to fight against counterfeiting and piracy. For example, ACTA attempts to enforce any use of a copyrighted work in the digital environment, without affording the recognized problem of lack of harmonization in either limitation or exception to intellectual property rights and the exhaustion of those rights.

Intellectual property rights are essentially private rights and hardly can override the rights to privacy and personal data protection, which have an intrinsic social value, particularly in democratic societies. Hardly, but not impossibly. Unfortunately, ACTA makes mistakes when it overrides its own purpose, by unnecessary diminishing the right to privacy and the right to protection of personal data, to provide enforcement not against smugglers and pirates, but against ordinary citizens.