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

ALBERTO J. CERDA SILVA*

* Professor, University of Chile Law School, acerda@uchile.cl.

INTRODUCTION

Globalization, digitalization, and the Internet have been the main challenges for intellectual property ("IP") since the turn of the century. Globalization has reduced the cost of transportation and communication across the world; the digitalization of content has facilitated and increased the flow of copyrightable works;[1] and, the Internet, which is the paradigm for global services, has allowed the cross-border transfer of digital works in seconds.[2] As a result of these phenomena, creating and maintaining an adequate protection for IP rights has required several modifications to both domestic and international laws, especially in regard to copyright.[3]

Until recently, at the international level, instruments on IP had focused their efforts on harmonizing domestic laws through the adoption of common standards on the scope, duration, and limitations of IP rights.[4] Therefore, to some extent, these instruments had ignored two issues: (1) the enforcement of those rules and (2) their adequacy for the digital environment. These issues, as well as the counterfeiting and piracy of goods that affect commercial interests, are the main topics addressed by the Anti-Counterfeiting Trade Agreement ("ACTA").

1. *See generally* NICHOLAS NEGROPONTE, BEING DIGITAL 58-61 (1995) (arguing that copyright law is inadequate to protect digital works because digitalization has become so precise, quick, and pervasive that it cannot be analogized to the copying of analog works).

2. *See* MARGARET JANE RADIN ET AL., INTERNET COMMERCE: THE EMERGING LEGAL FRAMEWORK 460 (Foundation Press, 2d ed. 2006) (noting that copyright owners initially hesitated to place their creations on the Internet because perfect copies could be disseminated quickly and easily).

3. *See id.* at 460-61 (commenting that technological innovations have led judges and legislators to update outdated language in court rulings and statutes).

4. *Cf.* Margot Kaminski, *The Origins and Potential Impact of the Anti-Counterfeiting Trade Agreement (ACTA)*, 34 YALE J. INT'L L. 247, 248 (2009) (noting that the World Intellectual Property Organization—based on the Paris and Berne Conventions—"served as a venue for treaty negotiation and soft law rather than a source of uniform standards or enforcement measures").

This article analyzes ACTA provisions that attempt to balance the protection of IP rights with the fundamental rights of users, in particular those related to the right to privacy and the right to protection of personal data.[5] As described in detail below, this work concludes that the ACTA negotiating parties ultimately failed to strike a balance that adequately protects such rights.

I. ACTA'S PURPOSE AND PRIVACY PROVISIONS

According to statements from governments taking part in the ACTA negotiations, the initiative aims to establish international standards for the enforcement of IP rights that target more efficiently the increasing problem of counterfeiting and piracy.[6] This effort is said to be focused on "commercially-oriented counterfeiting and piracy" rather than the activities of common people.[7] However, an analysis of ACTA's privacy provisions reveals a different concern; the provisions seem to focus more on enforcing the law against citizens rather than against large-scale criminal organizations.[8] The preamble of the finalized text of ACTA takes note of "the proliferation of . . . services that distribute infringing material" in

5. *See* discussion *infra* Part II (arguing that the standards established by ACTA will unjustifiably encroach upon citizens' civil rights).

6. *E.g.*, *ACTA Fact Sheet (March 2010)*, OFF. U.S. TRADE REPRESENTATIVE, http://www.ustr.gov/acta-fact-sheet-march-2010 (last visited Mar. 1, 2011).

7. *See id.* ("The ACTA does not focus on private, non-commercial activities of individuals, nor will it result in the monitoring of individuals or intrude in their private sphere."); *see also* Press Release, European Comm'n Directorate Gen. for Trade, Anti-Counterfeiting Trade Agreement: European Commission Welcomes Release of Negotiation Documents (April 21, 2010), http://trade.ec.europa.eu/doclib/press/index.cfm?id=552 (stating that ACTA's purpose is to "address large-scale infringements of intellectual property rights" and "by no means [will] lead to a limitation of civil liberties or to 'harassment' of consumers.").

8. *See, e.g.*, *infra* notes 112-116 and accompanying text; *see also* Kaminski, *supra* note 4, at 250 (implying that it is dangerous to conflate the terms "counterfeiting" and "copyright infringement," as this tends to lump dangerous counterfeiting, such as that linked to terrorism or the drug trade, in with less egregious individual instances of copyright infringement). *But see* Charles R. McManis, *The Proposed Anti-Counterfeiting Trade Agreement (ACTA): Two Tales of a Treaty*, 46 HOUS. L. REV. 1235 (2009) (describing "two tales" of the reasons for ACTA—(1) the need to fight organized crime and terrorist organizations, as representatives involved have claimed the agreement was meant to do, and (2) criminalizing file-sharing, as the drafts prior to the December 3, 2010 finalized version have indicated ACTA will attempt to do).

addition to counterfeiting and piracy, and expresses the desire to address that infringement.[9] This wording, which appears only in the Oct. 2, 2010 draft and the Dec. 3, 2010 final version,[10] painfully reveals the actual intent of the negotiating parties—to deal with the daily activities of common people.

Although the negotiations of ACTA did not take place in any multilateral forum[11] such as under the auspices of the World Trade Organization ("WTO") or the World Intellectual Property Organization ("WIPO"), the negotiations involved a cadre of states including Australia, Canada, Japan, Mexico, Morocco, New Zealand, Singapore, South Korea, Switzerland, the United States, and the European Union ("E.U.").[12] From 2008 to September 2010, there were eleven rounds of negotiations, all conducted secretly. Only after enormous pressure from civil society organizations and the European Parliament[13] was there an official public release of a provisional text

9. Anti-Counterfeiting Trade Agreement pmbl., Dec. 3, 2010 [hereinafter ACTA Text—Dec. 3, 2010], *available at* http://www.dfat.gov.au/trade/acta/Final-ACTA-text-following-legal-verification.pdf.

10. The recognition that the ACTA intended to deal with any infringement, and not only with piracy, started to appear in the October 2, 2010 draft. *Compare* Anti-Counterfeiting Trade Agreement: Informal Predecisonal/Deliberative Draft pmbl., Aug. 25, 2010 [hereinafter ACTA Draft—Aug. 25, 2010], *available at* https://sites.google.com/site/iipenforcement/acta (follow "Full Leaked Text Dated August 25, 2010") (discussing only the proliferation of counterfeit trademark and pirated copyright goods), *with* Anti-Counterfeiting Trade Agreement: Informal Predecisonal/Deliberative Draft pmbl., Oct. 2, 2010 [hereinafter ACTA Draft—Oct. 2, 2010], *available at* http://trade.ec.europa.eu/doclib/docs/2010/october/tradoc_146699
.pdf (including distributing services), *and* ACTA Text—Dec. 3, 2010, *supra* note 9, pmbl. (retaining the language regarding distributing services from the October 2, 2010 draft).

11. Eddan Katz & Gwen Hinze, *The Impact of the Anti-Counterfeiting Trade Agreement on the Knowledge Economy: The Accountability of the Office of the U.S. Trade Representative for the Creation of IP Enforcement Norms Through Executive Trade Agreements*, 35 YALE J. INT'L L. ONLINE 24, 26 (2009), http://www.yjil.org/online/volume-35-fall-2009/the-impact-of-acta-on-the-knowldge-economy (suggesting that the parties chose to negotiate outside of multilateral institutions because the institutions lack enforcement power).

12. Press Release, Office of the U.S. Trade Representative, U.S., Participants Finalize Anti–Counterfeiting Trade Agreement Text (November 15, 2010), http://www.ustr.gov/about-us/press-office/press-releases/2010/november/us-participants-finalize-anti-counterfeiting-trad.

13. *See, e.g.*, Resolution of 10 March 2010 on the Transparency and State of Play of the ACTA Negotiations, EUR. PARL. DOC. P7_TA-PROV(2010)0058

of the agreement—on April 21, 2010.[14] Unfortunately, this release was not much of a concession in favor of transparency concerns; the public had to wait until October 2, 2010 for the next official release, and until Dec. 3, 2010 for the release of the final draft text.[15] However, versions of the draft of the agreement were leaked: one before the first public release in January 2010[16] and others after the ninth and the tenth rounds in July[17] and August 2010,[18] respectively. Therefore, an inquiry into the negotiation and the developing interpretation of ACTA reveals that there is no public record of the successive rounds, save two official drafts, three leaked versions, and the final draft text. These documents expose an incomplete mosaic of the progress during the negotiations. This is especially the case for the leaked versions of the agreement, as they, unlike the official releases, include the positions of negotiators from specific countries and uncensored footnotes. This article is based on the final text of ACTA from December 3, 2010; consequently, all below references to the ACTA text are to the December 3, 2010 version, except as otherwise noted.[19]

(2010), *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 (reprimanding the European Commission for failing to inform or consult with Parliament about the negotiations, and threatening to bring a case before the European Court of Justice if the Commission continued to negotiate without transparency).

14. Anti-Counterfeiting Trade Agreement: Public Predecisonal/Deliberative Draft, Apr. 21, 2010 [hereinafter ACTA Draft—Apr. 21, 2010], *available at* http://trade.ec.europa.eu/doclib/docs/2010/april/tradoc_146029.pdf.

15. ACTA Draft—Oct. 2, 2010, *supra* note 10; ACTA Text—Dec. 3, 2010, *supra* note 9; *see* Press Release, Office of the U.S. Trade Representative, *supra* note 12 (emphasizing that despite the release of the final ACTA draft, the finalized version would still be subject to domestic processes).

16. Anti-Counterfeiting Trade Agreement: Informal Predecisonal/Deliberative Draft, Jan 18, 2010 [hereinafter ACTA Draft—Jan. 18, 2010], *available at* https://sites.google.com/site/iipenforcement/acta (follow "Full Leaked Text Dated January 18, 2010").

17. Anti-Counterfeiting Trade Agreement: Informal Predecisonal/Deliberative Draft, July 1, 2010 [hereinafter ACTA Draft—July 1, 2010], *available at* https://sites.google.com/site/iipenforcement/acta (follow "Consolidated ACTA Text, July 1, 2010").

18. ACTA Draft—Aug. 25, 2010, *supra* note 10.

19. In spite of the triumphalism that surrounded negotiators—who in October 2010 assured ACTA was done and required only that the parties sign it—the agreement still remained incomplete, to some extent. It required not only editing (e.g., there were still six articles numbered 2.X in that text), but also substantive

The structure of ACTA includes a preamble and six chapters covering initial provisions and definitions, proposed legal framework for the enforcement of IP rights, enforcement practices and mechanisms, norms of international cooperation, an institutional arrangement, and final provisions related to the effects of the agreement.[20] For purposes of this article, it is necessary to explain in some detail those norms related to the legal framework for enforcing the law, which include some general obligations, provisions on civil enforcement, border measures, criminal enforcement, and special measures related to the enforcement of IP rights in the digital environment.

The section on general obligations ensures the adoption of procedures by the parties and provides some general safeguards with several purposes, such as to avoid the abuse of procedures, to prevent public officers' liability, and others.[21]

In relation to civil enforcement, ACTA requires parties to have available civil procedures to enforce rights, including procedures for injunctions, damages, other remedies, access to information related to infringements and the people involved, and provisional measures.[22]

The section related to border measures requires parties to adopt certain measures for goods suspected of infringing IP rights, except in the case of de minimis infringement.[23] These measures can be adopted by application of rights holders or *ex officio* by custom authorities of member states,[24] for imported and exported goods, as

decisions related to the nature of some obligations of the parties (e.g., art. 2.14.3), safeguard measures (e.g., arts. 2.X: scope of the border measures, and 2.X: border measures), and more importantly the very scope of some provisions of the agreement (e.g., art. 2.18 and the still-in-bracket footnote 2). In fact, the same ACTA draft recognized that delegations had even expressed some reservations. *See* ACTA Draft—Oct. 2, 2010, *supra* note 10. Those pendent issues were solved only in the final text, ACTA Text—Dec. 3, 2010, *supra* note 9, which is analyzed in this article.

20. ACTA Text—Dec. 3, 2010, *supra* note 9.

21. *See id.* art. 6.

22. *Id.* arts. 7-12.

23. *See id.* art. 14, ¶ 2 (allowing parties to exempt from punishment travelers who possess a small number of non-commercial goods within their personal luggage).

24. Id. art. 16, ¶ 1; *see* T. Jesse Goff, Note, *Regulation of Digital Copyrights and Trademarks at the U.S. Border: How the Proposed Anti-Counterfeiting Trade*

well as those in transit or under customs control.[25] Parties shall also provide safeguard measures—procedures to determine infringement, remedies, and reasonable enforcement fees, and to some extent, the disclosure of information about infringements and the people involved.[26]

Although ACTA failed to conceptualize criminal offenses, it adopted a minimal common standard for criminal enforcement and allowed countries to heighten this standard.[27] This approach could be troublesome for those countries that limit criminal enforcement to for-profit infringements. Also, ACTA disproportionately extends liability to aiding and abetting,[28] and allows legal persons to be criminally liable without prejudice to the criminal liability of the natural persons involved in the offences.[29] In addition, ACTA adopts criteria for penalties and sanctions, and includes provisions about seizure, confiscation/forfeiture, and destruction of suspected counterfeit or pirated goods.[30] Finally, ACTA requires parties to allow *ex officio* criminal enforcement in established cases.[31]

The section on enforcement of IP rights in the digital environment is by far the most innovative,[32] as several of the issues raised by

Agreement and the Enacted U.S. Pro-IP Act will Destabilize the Current System, 16 SW. J. INT'L L. 207, 218-19 (2010) (contending that these provisions give customs officials an unnecessary amount of power to act on their own without any oversight).

25. ACTA Text—Dec. 3, 2010, *supra* note 9, art. 16, ¶ 2.

26. *Id.* arts. 18-22.

27. *Id.* art. 23, ¶ 1-3.

28. ACTA Text—Dec. 3, 2010, *supra* note 9, art. 23, ¶ 4; *cf. Anti-Counterfeiting Trade Agreement*, PUB. KNOWLEDGE, http://www.publicknowledge.org/anti-counterfeiting-trade-agreement (last visited Mar. 1, 2011) (proclaiming that the damages established by the agreement, which include imprisonment and monetary fines, are disproportionate to the crimes charged and do not include safeguards for innocent infringement).

29. ACTA Text—Dec 3, 2010, *supra* note 9, art. 23, ¶ 5.

30. *Id.* arts. 24 & 25.

31. *Id.* art. 26; *see* Goff, *supra* note 24, at 220 (pointing out that the civil liberties group IP Justice has harshly criticized *ex officio* criminal enforcement because it violates an alleged infringer's due process right to challenge an official's accusation of infringement and decision to seize and destroy the alleged infringer's property).

32. *See* McManis, *supra* note 8, at 1253 (remarking that the provisions regarding Internet regulation were highly controversial because they proposed monitoring citizens and internet service providers, which detracts from ACTA's original focus on commercial activity).

those provisions have never been regulated in previous international instruments, not even in the WIPO Internet Treaties.[33] This section seems to be drafted as an updated version of the Digital Millennium Copyright Act ("DMCA"),[34] but, by the July 1, 2010 draft, there was evident disagreement among the parties. In fact, almost all the articles were still in brackets (meaning they were not agreed upon), several included alternate proposals, and the section contained more footnotes than any other.[35] Scholars and civil society organizations seriously criticized the intended provisions for disrespecting human rights standards, damaging IP balances, and undermining the capacity of countries to adopt and implement policies of public interest.[36] Unable to harmonize different legal regimes, negotiators made key concessions during the last two draft rounds by (1) refraining from settling on provisions about the limitation of liability for online service providers, and (2) lowering their expectations for protection of effective technological measures and rights management information.[37]

33. Kaminski, *supra* note 4, at 247-48. The World Intellectual Property Organization adopted both the Performances and Phonograms Treaty and the Copyright Treaty, collectively known as the WIPO Internet Treaties, which provide protection for works in the digital environment and regulate technological protective measures. *See* World Intellectual Property Organization Performances and Phonograms Treaty, art. 18, Dec. 20, 1996, S. TREATY DOC. NO. 105-17 (1997); World Intellectual Property Organization Copyright Treaty, Dec. 20, 1996, S. TREATY DOC. NO. 105-17 (1997).

34. 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 limiting the liability of online service providers for copyright infringement. *See* Digital Millennium Copyright Act, Pub. L. No. 105-304, 112 Stat. 2860 (1998) (codified in scattered sections of 17 U.S.C. and 28 U.S.C.).

35. *See* ACTA Draft—July 1, 2010, *supra* note 17, art. 2.18 & n.44 (containing conflicting suggestions and revisions from eleven separate parties with some, including Canada and Mexico, reserving the right to make more adjustments at a later date).

36. *See, e.g.*, *Text of Urgent ACTA Communique: International Experts Find that Pending Anti-Counterfeiting Trade Agreement Threatens Public Interests*, AM. U. WASH. C. L. PROGRAM ON INFO. JUST. & INTELL. PROP. (June 23, 2010), http://www.wcl.american.edu/pijip/go/acta-communique [hereinafter *Urgent ACTA Communique*] (concluding that the April 2010 ACTA draft contained provisions that are hostile to the public interest because they limited basic human rights for the protection of personal data and freedom of expression, among others).

37. *Compare* ACTA Draft—July 1, 2010, *supra* note 17, art. 2.18 (suggesting language that would generally exempt service providers from liability where the

In the finalized text of ACTA, the section on the enforcement of IP rights in the digital environment, the scope of which is ambiguous,[38] begins by establishing an unwieldy complementary application of the provisions related to civil and criminal enforcement.[39] The section then requires promoting cooperation within the business community to address IP infringement,[40] encourages the disclosure of personal information of Internet users by online service providers,[41] and mandates protection of effective technological measures and electronic rights management information.[42]

Unlike previous international agreements on IP, 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.[43] The Agreement on Trade-

infringement results from automated technology, is uploaded by a user and not the service provider, or a user posts a link to a site with infringing material), *with* ACTA Text—Dec. 3, 2010, *supra* note 9, art. 27 (dropping these specific provisions).

38. Even by the last round of negotiations, some delegations had expressed reservations around several provisions of this section, which remained pendent. *Compare* ACTA Draft—Oct. 2, 2010, *supra* note 10, art. 2.18 (suggesting a broad scope that included all intellectual property rights in the title of the section and its article 2.18.1; the existence of competing proposals for articles 2.18.2 to 2.18.4, one limiting the effects to copyright and related rights, while another extending its scope *at least* to trademark and copyright and related rights), *with* ACTA Text—Dec. 3, 2010, *supra* note 9, art. 27 (preserving a broad scope for the provisions in the name of the section title and art. 27 ¶¶ 1 and 2; narrowing the scope to trademark, copyright and related rights, in art. 27 ¶¶ 3 and 4; and, limiting its effects to copyright and related rights, in art. 27 ¶¶ 5-8)

39. *See* ACTA Text—Dec. 3, 2010, *supra* note 9, art. 27, ¶ 1 (applying to the digital environment the enforcement procedures set forth in Sections 2 and 4 of the agreement without regard to the unique circumstances of that environment).

40. *Id.* art. 27, ¶ 3.

41. *Id.* art. 27, ¶ 4.

42. *Id.* art. 27, ¶¶ 5-7. The agreement requires the prohibition of manufacturing, importing, or distributing devices or services that are primarily designed to circumvent rights protections or has limited commercial significance outside of such a function. *Id.* ¶ 6. The agreement also allows certain "appropriate" exceptions to "measures implementing the provisions" dealing with effective technological measures. *Id.* ¶ 8.

43. *See* Berne Convention for the Protection of Literary and Artistic Works, Sept. 9, 1886, *as amended on* Sept. 28, 1979, 25 U.S.T. 1341, 1161 U.N.T.S. 30;

Related Aspects of Intellectual Property Rights ("TRIPS Agreement") refers to such protection only indirectly; it provides that members of the World Trade Organization ("WTO") may allow their judicial authorities to order alleged infringers to disclose the identity of third persons involved in infringements, but only when such disclosure would not be disproportionate to the seriousness of the infringement.[44] In addition, the TRIPS Agreement includes some provisions that deal with secrecy and confidentiality, but they focus on commercial, business, and manufacturing information, not on personal information.[45]

ACTA expressly calls attention to privacy and data protection in several of its provisions by ensuring that nothing in ACTA detracts from domestic legislation regarding the protection of the right to privacy.[46] In particular, it does not preempt domestic laws that regulate access to or disclosure of personal data in civil enforcement and border measures;[47] it encourages parties to order online service providers ("OSPs")[48] to transfer expeditiously information on the

Paris Convention for the Protection of Industrial Property, Mar. 20, 1883 (as last revised at Stockholm, July 14, 1967), 21 U.S.T. 1583, 828 U.N.T.S. 305.

44. Agreement on Trade-Related Aspects of Intellectual Property Rights, art. 47, Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1C, 1869 U.N.T.S. 299 [hereinafter TRIPS Agreement].

45. *See, e.g.*, *id.* art. 34, ¶ 3 (ensuring that parties take into account the need to protect manufacturing and business secrets when establishing the burden of proof for process patents); *id.* art. 39, ¶ 3 (prohibiting parties from disclosing chemical patent information unless necessary to protect the public or where parties ensure the information is not utilized for unfair commercial purposes); *id.* art. 40 (protecting the confidentiality of information when nations work in conjunction to control anti-competitive practices); *id.* arts. 42-43 (mandating the creation of evidentiary procedures to identify and protect confidential information in the enforcement of intellectual property rights); *id.* art. 57 (exempting measures for the "protection of confidential information" from customs searches); *id.* art. 63, ¶ 4 (safeguarding confidential information from transparency requirements).

46. *See, e.g.*, ACTA Text—Dec. 3, 2010, *supra* note 9, art. 4 (limiting the disclosures of confidential information to the level allowed under each party's privacy laws).

47. *Id.* art. 22.

48. Unlike the more popular phrase "Internet service provider" ("ISP"), "online service provider" suggests that the provisions apply not only to those that offer services through the Internet, but any public or private, open or closed digital network. Because of that difference in the intended scope and because of its actual use in all ACTA drafts, this paper adopts it, despite American readers likely being less familiar with it than the ISP phrase.

identity of subscribers to right holders in claims of infringement;[49] and it preserves privacy in the implementation of enforcement procedures, cooperation within the business community, and the identification of Internet users.[50] In addition to these express mentions, ACTA suggests a connection with the right of privacy in several other provisions, such as those referring to the rights of participants in procedures, preservation of evidence, collection, analysis and cross-border transfer of relevant data, and information sharing through international cooperation.[51] Therefore, ACTA both expressly and implicitly references the right to privacy.

The Executive Director of the Electronic Privacy Information Center, Marc Rotenberg, correctly states that IP rights never have conferred *per se* the right to identify users.[52] However, because enforcing IP rights requires identifying supposed infringers, particularly in the digital environment, the ACTA negotiating parties have been forced to include the aforementioned provisions about privacy and personal data protection. The provisions seemingly intend to balance competing interests—reaching an appropriate level of enforcement for IP and, at the same time, guaranteeing an adequate level of protection for privacy and personal data. Such a balance is elusive, particularly because the underlying interests conflict.[53] In spite of their social value as promoters of the progress

49. *Id.* art. 27, ¶ 4.

50. *Id.* art. 27, ¶¶ 2-4 (adding that these obligations shall be implemented in a "consistent [manner] with that Party's law, [and] preserve[] fundamental principles such as freedom of expression, fair process, and privacy").

51. *See, e.g.*, *id.* art. 12, ¶ 4 (requiring a party to provide assistance to a defendant to prevent the abuse of a defendant's rights); *id.* art. 14, ¶ 2 (permitting the exclusion of personal non-commercial infringing goods from a party's rules); *id.* art. 28, ¶ 4 (promoting the collection and analysis of data); *id.* art 34 (mandating information sharing between parties).

52. *See* The WIPO Copyright Treaties Implementation Act and Privacy Issues: Hearing on H.R. 2281 Before the Subcomm. on Telecomms., Trade, and Consumer Prot. of the House Comm. on Commerce, 105 Cong. (1998) [hereinafter WIPO Copyright Treaty Hearing] (testimony and statement of Marc Rotenberg, Dir., Electronic Privacy Info. Ctr.) (observing that the protection of copyright ownership did not threaten privacy protections historically).

53. *See id.* (acknowledging that it may be necessary to identify the user of a work to establish infringement, but arguing that information should not be collected on individuals' personal Internet activities and private preferences or people may be forced to avoid the Internet to protect their privacy).

of science and useful arts,[54] IP rights are essentially "private rights."[55] Obtaining adequate protection for the rights to privacy and personal data is important not just for individual interests, but also for the protection of higher societal values. The rights to privacy and personal data are essential to the very idea of democracy and as safeguards of human rights.[56]

In the following pages, this article briefly analyzes the main challenges that ACTA creates for privacy and data protection, nascent provisions for an international treaty about IP. Unfortunately, the numerous references to privacy and personal data protection in the treaty does not mean that ACTA strikes an adequate balance between the interests at play. In fact, this article concludes the opposite—that ACTA has seriously undermined the right to privacy and the protection of personal data.

II. CRITICISMS OF ACTA'S PRIVACY PROVISIONS

Analyzing the effects of ACTA on privacy and data protection poses some challenges. Luckily, with the completed agreement, they are less daunting now as compared to months ago when the draft was replete with brackets, proposals, and footnotes, which indicated dissimilar positions and prevented identifying the real intent of the negotiating parties, let alone which provisions would ultimately prevail. However, the main challenge in analyzing ACTA persists; that is, the lack of official reports on the meetings and the secrecy of the negotiations have obstructed any effort to discern the actual public policy rationale for the decisions taken by negotiating parties, especially given the remaining ambiguities and remarkable omissions.[57]

54. *See* U.S. CONST. art. I, § 8 ("The Congress shall have power To . . . promote the Progress of Science and useful Arts, by securing for limited Times to Authors and Inventors the exclusive Right to their respective Writings and Discoveries.").

55. TRIPS Agreement pmbl. ("recognizing that intellectual property rights are private rights").

56. *Cf.* Frances S. Grodzinsky & Herman T. Tavani, *P2P Networks and the* Verizon v. RIAA *case: Implications for Personal Privacy and Intellectual Property*, 7 ETHICS & INFO. TECH. 243 (2005) (arguing that privacy protections are necessary for the preservation of individual autonomy and to enable free expression).

57. *See, e.g.*, Katz & Hinze, *supra* note 11, at 30-31 (revealing that the U.S.

Probably because the E.U. has the strongest legal framework for the protection of rights to privacy and personal data,[58] its authorities criticized ACTA for failing to provide adequate protection to those rights; this criticism lead the negotiators to introduce most of the clauses that are intended to safeguard the aforementioned rights and to reject some of the proposed clauses that jeopardized them.[59] Analyzing, or even describing, the legal framework to protect privacy and personal data adopted by the E.U. is beyond the scope of this paper. But, briefly, their framework provides a comprehensive legal regime for processing personal data related to physical persons, by automatic or manual process, for the public and private sectors.[60] At the Community level, this framework includes specific provisions in the Charter of Human Rights[61] and several directives, such as the Data Protection Directive,[62] the Directive on Privacy and Electronic Communications,[63] and the Data Retention Directive.[64] As a general principle, the processing of personal data requires the express consent of the data subject, except in specific circumstances provided by domestic law, and the independent national authorities' guarantee of the enforcement of the law.[65]

In February 2010, one month after the first leaked version of

Trade Representative vehemently protected the information and requested that the negotiation participants sign a confidentiality agreement and that little information be released to the public, possibly to avoid the backlash such analysis could create).

58. *See* Fred H. Cate, *The EU Data Protection Directive, Information Privacy, and the Public Interest*, 80 IOWA L. REV. 431, 437-39 (1995) (noting that European Union countries have provided such significant data protection that they have pressured the United States and Canada to improve theirs, which, at the time this article was written, was virtually nonexistent).

59. This point is particularly evident when contrasting the outcome drafts from the ninth and the tenth rounds of negotiation, that is, between June and August 2010. *Compare* ACTA Draft—July 1, 2010, *supra* note 17, *with* ACTA Draft—Aug. 25, 2010, *supra* note 10.

60. Council Directive 95/46, art. 3.1, 1995 O.J. (L 281) 31 (EC).

61. Charter of Fundamental Rights of the European Union, art. 8, 2000 O.J. (C 364) 1.

62. Council Directive 95/46, *supra* note 60.

63. Council Directive 2002/58, 2002 O.J. (L 201) 37 (EC).

64. Council Directive 2006/24, art. 1.1, 5, 2006 O.J. (L 105) 54 (EC).

65. *See* Cate, *supra* note 58, at 433 (elaborating that the processing of personal data may occur in three situations: (1) with consent; (2) when data is legally required to be processed; and (3) to protect the public interests of a private party holding certain fundamental rights).

ACTA, the European Data Protection Supervisor ("Supervisor") issued an opinion expressing his concerns about potential incompatibility between envisaged ACTA measures and the requirements of the E.U.'s data protection law.[66] The Supervisor drew special attention to the provision dealing with the three strikes policy, which encourages the disconnection of users from the Internet for supposed IP infringements, and the transfer of personal data to third-party countries (i.e., states outside the E.U.) for purposes of IP enforcement.[67] Later, in July 2010, the Data Protection Working Party ("WP29"), which is integrated with the national authorities on the matter, sent a public letter to the European Commission. In its letter, the WP29 called attention to several of the proposed ACTA measures that interfered with the right to privacy, expressing unease over future negotiations.[68] This article returns to the concerns of the E.U. authorities throughout the below analysis.

The following pages describe the provisions of ACTA related to privacy and personal data, show how they connect with IP enforcement, and analyze how they challenge the legal regimes in countries that have already afforded some protection to privacy and personal data.

A. ACTA MAKES A SERIOUS AND UNPRECEDENTED CONCESSION OF PRIVACY AND DATA PROTECTION IN FAVOR OF INTELLECTUAL PROPERTY ENFORCEMENT

As aforementioned, ACTA makes several direct and indirect references to privacy and data protection in an attempt to strike a

66. Opinions of the European Data Protection Supervisor on the Current Negotiations by the European Union of an Anti-Counterfeiting Trade Agreement (ACTA), 2010 O.J. (C 147) ¶¶ 3, 8 [hereinafter Data Protection Supervisor Opinions] (observing that intellectual property rights enforcement may threaten individuals' "fundamental right" to privacy and the protection of personal information).

67. *Id.* ¶¶ 3-13.

68. *See* Letter from the Article 29 Data Protection Working Party to Karel de Gucht, Comm'r, Eur. Comm'n, regarding the Data Protection and Privacy Implications of the Anti-Counterfeiting Trade Agreement [ACTA] (July 15, 2010) [hereinafter Letter from WP29], *available at* http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/others/2010_07_15_letter_wp_commissioner_de_gucht_acta_en.pdf. (identifying the three strikes scheme, notice and take down procedure, and searches by customs authorities as measures that would interfere with privacy rights).

balance with IP enforcement. The very mention of these interests could be understood as an achievement for privacy advocates because ACTA is the first international IP agreement to explicitly recognize the importance of privacy and data protection. However, in comparing ACTA with the TRIPS Agreement, those references seem to be a mere concession in favor of IP enforcement.

In effect, the TRIPS Agreement recognizes not only the relevant international IP agreements and conventions, but also the applicability of the basic principles of the General Agreement on Tariffs and Trade ("GATT") of 1994 and the General Agreement on Trade in Services ("GATS"), which are the multilateral treaties that set forth rules governing international trade in goods and services enforced by the WTO.[69] The latter includes general exceptions that authorize measures inconsistent with GATS when those measures are necessary to secure compliance with laws or regulations related to the protection of individual privacy.[70] These general exceptions allow countries to develop public policies on several issues without practical limitations in fields such as safety, protection of the environment, public morals, public order, and personal data protection.[71] ACTA, on the contrary, requires countries to adopt given measures against the privacy and personal data protection of Internet users in order to enforce IP laws,[72] such as encouraging their identification by OSPs and requiring the cross-transfer of personal

69. *See Intellectual Property: Protection and Enforcement*, WORLD TRADE ORG., http://www.wto.org/english/thewto_e/whatis_e/tif_e/agrm7_e.htm (last visited Mar. 1, 2011) (noting that in addition to the basic principles contained in GATT and GATS, the TRIPS Agreement includes the principle of contribution to technical innovation and transfer of technology).

70. *See* General Agreement on Trades in Services, art. XIV, Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1B, 1869 U.N.T.S. 183 [hereinafter GATS] (applying these exceptions in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts).

71. *See* PETER P. SWIRE & ROBERT E. LITAN, NONE OF YOUR BUSINESS: WORLD DATA FLOWS, ELECTRONIC COMMERCE, AND THE EUROPEAN PRIVACY DIRECTIVE 191 (1998) (explaining limitations to the exception, none of which refer to intellectual property enforcement). In fact, countries using this exception abide by several tests set forth by Article XIV of the GATS, and thereby prevent abuse of the exceptions. *See* Council for Trade in Services, Work Program on Electronic Commerce, *Progress Report to the General Council*, S/L/74, ¶ 14 (July 27, 1999).

72. *E.g.*, *Urgent ACTA Communique*, *supra* note 36.

data between states parties.[73] Neither the inclusion of safeguards in ACTA nor the express recognition of the freedom of parties to determine the appropriate method of implementation changes the fact that countries must adopt measures that undermine the rights to privacy and the protection of personal data.

In sum, ACTA has made a serious and unprecedented concession of privacy and data protection in favor of IP enforcement by depriving countries of the freedom to adopt laws protecting the rights to privacy and personal data protection, and by requiring the implementation of measures that will negatively affect those rights.[74] To be clear, ACTA does not prevent the adoption of public policies on privacy and data protection by countries, but certainly imposes some conditions on them.

B. ACTA OMITS APPROPRIATE SAFEGUARDS FOR THE RIGHT TO PRIVACY IN GENERAL

Given the broad concession that ACTA has made with rights to privacy and the protection of personal data in favor of IP enforcement, it was necessary for the negotiating parties to include appropriate limitations and safeguards for such rights because other international instruments covering IP lack such protections. Even though international instruments on human rights already protect the right to privacy and the right to personal data protection, their effects are limited, and none clearly apply to the possible abusive enforcement of IP laws. Indeed, some have limited personal effect, such as the Charter of Fundamental Rights of the European Union,[75] and most are not legally binding[76] and, therefore, almost impossible

73. ACTA Text—Dec. 3, 2010, *supra* note 9, arts. 29 ¶ 1(b), 33 ¶ 3, 34.

74. *See* Goff, *supra* note 24, at 219-20 (indicating that ACTA privacy protections are likely insufficient because the agreement encourages nations to share information with one another, thereby mooting domestic regulations on obtaining information).

75.*See* Charter of Fundamental Rights of the European Union, arts. 7-8, 2000 O.J. (C 364) 1 (providing that the right to privacy and the right to protection of personal data shall be protected, but not addressing the competing interest of enforcing intellectual property rights).

76. *See, e.g.*, United Nations Guidelines Concerning Computerized Personal Data Files, G.A. Res. 45/95, U.N. Doc. A/RES/45/95 (Dec. 14, 1990) (calling for governments to consider including the guidelines for computerized personal data files in their domestic laws); ASIA-PACIFIC ECON. COOPERATION, PRIVACY

to enforce.[77] Others could be legally binding but have an extremely generic and ambiguous enunciation of those rights.[78] In some countries, like in the United States, human rights in general have limited enforcement against the private sector, such as right holders and service providers.[79] Therefore, it was essential to include some provisions that balance the right to privacy and IP enforcement.

During most of the negotiations, ACTA lacked any general provision intended to deal with this balance. Only in the ninth round of negotiations, which seems quite late given the importance of this issue—particularly for the E.U., were different safeguards included among the initial provisions.[80] Most of them did not make it into the final draft, but two provisions did survive and are particularly relevant for purpose of this paper. According to ACTA:

> "Nothing in this Agreement shall require any Party to disclose: (a) information the disclosure of which would be contrary to its law or its international agreements, including laws protecting privacy rights . . .; (b) confidential information, the disclosure of which would impede law enforcement or otherwise be contrary to the public interest . . . ."[81]

FRAMEWORK ¶ 12 (2005), *available at* http://www.ag.gov.au/www/agd/rwpattach.nsf/VAP/%2803995EABC73F94816C2AF4AA2645824B%29~APEC+Privacy+Framework.pdf/$file/APEC+Privacy+Framework.pdf (explaining that members should have flexibility to implement the principles that best suit their economic and social backgrounds).

77. These instruments are only enforceable if they become customary norms. However, they currently exist as non-binding rules and mere recommendations for parties, lacking *opinio juris*, an essential element for customary law. *See, e.g.*, RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW §102 (1987) (defining customary international law as a widely accepted principle that is generally and consistently practiced by states out of a sense of legal obligation).

78. *See, e.g.*, Universal Declaration of Human Rights, G.A. Res. 217 (III) A, art. 12, U.N. Doc. A/RES/217(III) (Dec. 10, 1948) (setting forth a general rule that no one shall be subject to arbitrary interference with his privacy). This portion of the Universal Declaration of Human Rights was codified in the International Covenant on Civil and Political Rights, art. 17, Dec. 16, 1966, 999 U.N.T.S. 171.

79. However, remedies against private parties may be available. *See, e.g.*, Alien Tort Claims Act, 28 U.S.C. § 1350 (2006) (granting federal court jurisdiction for civil cases where an alien has violated international law); Torture Victim Protection Act of 1991, Pub. L. 102-256, 106 Stat. 73 (codifying the availability of civil damages for a torture victim against a perpetrator acting under actual or apparent authority of a foreign nation).

80. ACTA Draft—July 1, 2010, *supra* note 17, art. 1.4.

81. ACTA Text—Dec. 3, 2010, *supra* note 9, art. 4, ¶ 1 (containing an

A thoughtless reading of these two clauses might give the impression that they leave room for the parties to implement domestic privacy laws that conflict with other obligations set forth in ACTA; this is an effect similar to that of GATS, which safeguards some public policies that, in theory, are inconsistent with its own principles.[82] However, a more attentive reading reveals that these clauses have a narrow scope and objective. As will be analyzed later, these clauses deal only with the disclosure of information between parties; they do not deal with every process related to personal information, and they refer only to the disclosure of such information from one country to another.[83] As a result of those limitations, the mentioned clauses do not prevent abuse of IP enforcement and jeopardize privacy and personal data protection. ACTA therefore fails to provide an appropriate general safeguard for the rights to privacy and data protection.

C. ACTA ENCOURAGES STATES PARTIES TO GRANT GREATER ACCESS TO INTERNET USERS' PERSONAL INFORMATION THAN ALLOWED UNDER DOMESTIC LAWS IN FORCE

Enforcing the law in the digital environment to address individual infringement requires the identification of infringers and, consequently, collaboration between OSPs and rights holders. OSPs have been collecting and processing Internet users' personal data for a long time, initially for pricing purposes,[84] later by law in order to assist with criminal prosecutions—particularly of cyber crime.[85] By

additional third clause, which also sets forth an exception to the disclosure of information that deals with confidential information of particular enterprises).

82. *See supra* note 70 and accompanying text.

83. *See infra* Part II.G.

84. For example, before offering Internet service access on a flat rate basis, Internet service providers used a price structure based on the amount of time connected, a calculation requiring them to process Internet users' personal data. *See* Andrew Odlyzko, *Internet Pricing and the History of Communications* 5, 7 (AT&T Labs Research Paper, Feb. 8, 2001), *available at*, http://www.dtc.umn.edu/~odlyzko/doc/history.communications1b.pdf.

85. *See* Convention on Cybercrime, art. 20, Nov. 23, 2001, E.T.S. 185 (ordering parties to provide measures through which authorities can direct OSPs to collect or record Internet usage data). *But see* Susan W. Brenner, *The Council of Europe's Convention on Cybercrime*, *in* CYBERCRIME: DIGITAL COPS IN A NETWORKED ENVIRONMENT 207, 211-12 (Jack M. Balkin et al. eds., 2007) (arguing that parties of the Convention have been unable to adopt even a common

knowing the Internet protocol address[86] and the date and time of connection, OSPs are able to identify the connected computer. Once the connected computer is identified, it is possible to connect it to an Internet user and his/her physical address.[87]

Several provisions of ACTA require granting access to information that facilitates the identification of supposed IP infringers. Negotiators approved the inclusion of express privacy safeguards related to statutory provisions that regulate the processing of personal data;[88] however, in the case of the digital environment, a previous draft of ACTA emphasized that parties shall enable right holders to "expeditiously" obtain from OSPs the information necessary to identity the alleged infringer.[89] The final text of ACTA retains the "expeditious[]" language but does not oblige parties to enable such access to indentifying information.[90] In other words, the

understanding of 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).

86. An Internet protocol address is a number assigned to any device (i.e., a computer) connected to the Internet. *See Data Protection Supervisor Opinions*, *supra* note 66, ¶ 25. Sometimes the number varies according to the time of connection and is assigned on demand by the OSP. This is called a dynamic Internet protocol address. In other instances that number is permanently linked to a given device, known as permanent Internet protocol addresses. *Id.* ¶ 25 n.17.

87. *See id.* This tracking system allows the identification of computers rather than users. *Id.* ¶ 25. In fact, in some cases it is necessary to adopt additional technical measures to identify a user, such as in the case of an open network (e.g., universities use a user name and password, while cybercafés use registers for identifying users). *Cf. id.* (acknowledging that Internet protocol addresses and the information acquired about them, including the user's identity, constitutes personal data).

88. *See* ACTA Text—Dec. 3, 2010, *supra* note 9, art. 27, ¶ 4 (providing a general safeguard against violations of fundamental principles, including privacy, but not expressly stating that violations of privacy rights shall not be allowed). According to the first leaked version, those safeguards, which appear approved by the second leaked version, were promoted by the European Union. *See* ACTA Draft—Jan. 18, 2010, *supra* note 16, art. 2.4; ACTA Draft—July 1, 2010, *supra* note 17, art. 1.4.

89. ACTA Draft—Apr. 21, 2010, *supra* note 14, art. 2.18.3 *ter*.

90. ACTA Text—Dec. 3, 2010, *supra* note 9, art. 27, ¶ 4 ("Each party may provide . . . its competent authorities with the authority to order an online service provide to disclose expeditiously . . . information sufficient to identify an alleged infringer."). The change from a mandatory to a facultative provision must have happened between the April draft and August leak. *Compare* ACTA Draft—Apr. 21, 2010, *supra* note 14, art. 2.18.3 *ter* ("Each Party shall enable right holders . . .

"shall" became a "may." But still, rather than providing flexibility in its implementation, that language reflects the failure of the negotiating parties to reach a common understanding on the matter; in fact, many countries involved in the negotiations already have laws that allow the copyright holder to access such information from OSPs.[91] In any case, this discretionary language is dangerous, especially considering the excesses of ACTA and its insufficient safeguards and flexibilities,[92] because other countries may be politically compelled to adopt provisions already suggested by ACTA.

Furthermore, the text of ACTA creates uncertainty by failing to define "online service provider."[93] The obligation to identify subscribers applies to any OSP and, at least until July 2010, ACTA contained an extremely broad concept of an OSP.[94] In fact, that

to expeditiously obtain from [the relevant OSP] information on the identity of the [allegedly infringing] subscriber."), *with* ACTA Draft—Aug. 25, 2010, *supra* note 10, art. 2.18.4 (using the same language as is found in the December final draft).

91. *See, e.g.*, *Domestic Laws in ACTA-Negotiating Countries*, AM. U. WASH. C. L. PROGRAM ON INFO. JUST. & INTELL. PROP., https://sites.google.com/site/iipenforcement/domestic-laws-in-acta-negotiating-countries (last visited Mar. 1, 2011). There are such laws on the books of Australia, E.U. members, Korea, New Zealand, and the United States, but, for example, Mexico does not have legal provisions related to the liability of online service providers for copyright infringement—neither notice-and-takedown procedures nor rules related to identifying subscribers. *Id.*

92. *See infra* Parts II.D-G.

93. *See USTR Releases Finalized ACTA Text: Concerns Remain*, PUB. KNOWLEDGE (Nov. 15, 2010, 9:41PM), http://www.publicknowledge.org/blog/ustr-releases-finalized-acta-text-concerns-re (warning that the failure to define "online service provider" could result in requiring websites that host content, such as YouTube, to identify subscribers as well).

94. *See, e.g.*, ACTA Draft—July 1, 2010, *supra* note 17, art. 2.18, ¶ 3 n.48 (conceptualizing an OSP as "a provider of online services or network access, or the operators of facilities therefore, [including] 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 users choosing, without modification to the content of the material as sent or received"). It seemed negotiating parties were in agreement on the definition of "online service provider," as, with the exception of a cosmetic Canadian proposal, no alternative proposal appeared in the July draft, and there is no record of serious opposition by any other country in any other draft. *See id.*; ACTA Draft—Jan. 18, 2010, *supra* note 16, art. 2.17, ¶ 3 n.26 (including the concerns of New Zealand and Japan, respectively, over whether "online service provider" includes a person who hosts materials online, and whether the definition as a whole is "acceptable"); ACTA

definition was broader than any other available in comparative law, as it applied to any person—including physical persons, to any provider—even those that only provide access, and, not only to Internet-based providers, but to any online service.[95] Fortunately, that definition was expunged from the text of ACTA, but, unfortunately, a new one was not substituted in its place. Therefore, ACTA offers no guidance on the meaning of the phrase "online service provider," and whether it meets the domestic legal standards in force among negotiating parties.

In the United States, DMCA procedures for taking down content and identifying users are limited to an OSP that is an "entity"[96]—that is, "an organization (such as a business or a governmental unit) that has a legal identity apart from its members."[97] In other words, those procedures apply only to legal persons, but not to physical persons or human beings. According to older ACTA drafts, those provisions would apply to any provider, which "*includes an* entity."[98] Therefore, at least in the case of the United States and countries that have adopted provisions similar to the DMCA in their Free Trade Agreements ("FTAs"),[99] the older ACTA drafts would have extended the duties, obligations, and costs of IP enforcement not just to legal persons, but possibly to common people. Today, because the latest ACTA draft lacks a definition at all, the extent of those duties, obligations, and cost is unclear.[100]

Draft—Apr. 21, 2010, *supra* note 14, art. 2.18, ¶ 3 n.50 (listing the proposed definition in brackets, but not including the negotiating parties' opinions of the definition). The definition was dropped for the August, October, and most recent December drafts. ACTA Draft—Aug. 25, 2010, *supra* note 10; ACTA Draft—Oct. 2, 2010, *supra* note 10; ACTA Text—Dec. 3, 2010, *supra* note 9.

95. ACTA Draft—July 1, 2010, *supra* note 17, art. 2.18, ¶ 3 n.48.

96. 17 U.S.C. § 512(k)(1) (2006).

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

98. *E.g.*, ACTA Draft—July 1, 2010, *supra* note 17, art. 2.18, ¶ 3 n.48.

99. The United States has included similar provisions in FTAs with Singapore, Chile, Morocco, Australia, Costa Rica, El Salvador, Guatemala, Honduras, Nicaragua and Dominican Republic, Bahrain, Oman, Peru, Colombia, and Panama. *See Free Trade Agreements*, U.S. TRADE REP., http://www.ustr.gov/trade-agreements/free-trade-agreements/free-trade-agreements (last visited Mar. 1, 2011).

100. *See Anti-Counterfeiting Trade Agreement*, *supra* note 28 (decrying the vagueness of ACTA and arguing that the agreement heightens IP enforcement without "even the barest measures to preserve" citizens' rights).

In the United States, according to the criterion in *Recording Industries Association of America v. Verizon Internet Services, Inc.*, DMCA procedures do not require mere internet access providers—companies that serve only as conduits to the Internet—to hand over information identifying alleged infringers.[101] Similarly, the E.U.'s E-Commerce Directive, which regulates the procedure by which users are identified, does not apply to mere providers of access, but to those that provide storage services.[102] ACTA's broad definition of "online service provider," to the extent it becomes part of the final treaty, would cause its user-identification procedures to apply to companies that serve only as access providers; ACTA neither makes any distinction related to this obligation nor to the kind of service provided by OSPs.[103]

The deleted definition of OSPs not only applied to any person and provider, even those that provide only access, but also to any online

101. 351 F.3d 1229, 1237 (D.C. Cir. 2003). Commentators agree that the Verizon case has been a triumph for privacy advocates, but it has not seriously affected the copyright holders' protections 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. *See, e.g.*, Alice Kao, RIAA v. Verizon*: Applying the Subpoena Provision of the DMCA*, 19 BERKELEY TECH. L.J. 405, 421-24 (2004) (discussing the potential for abuse in John Doe lawsuits, citing the provision's broad language, lack of judicial oversight, and the lack of a notice requirement); Tomas P. Owen, Jr. & 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, 623, 632-634 (2004) (approving of the John Doe subpoenas because they are not more expensive or time consuming than section 512(h) requests to subpoena service providers).

102. Directive 2000/31 of the European Parliament and of the Council of 8 June 2000 on Certain Legal Aspects of Information Society Services, 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 Telecommunicaion GmbH, 2009 O.J. (C 113) 14 (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 storage service).

103. *See* ACTA Draft—July 1, 2010, *supra* note 17, art. 2.18, ¶ 3 n.48 (defining an "online service provider" as *including* an entity—not limited to an entity). ACTA, however, did make that distinction in the proposed notice-and-take-down procedure. *See id.* art. 2.18, ¶ 3(b); *see also* ACTA Draft—Jan. 18, 2010, *supra* note 16, art. 2.17, ¶ 3 n.28 (excluding from the notice-and-take-down procedures those providers acting solely as a conduit for Internet access).

service, not only Internet-based providers. If this definition becomes part of the finalized text, it could be cumbersome for negotiating parties, and maybe even weaken domestic regulatory protections if the provision regarding the identification of alleged infringers reverts back to being mandatory rather than permissive. For example, E.U. law limits the collection of personal data generated or processed by "providers of publicly available electronic communications services or of a public communications network."[104] Therefore, ACTA could undermine this standard by imposing obligations on types of OSPs that are not yet addressed in the current E.U. law, such as private network services.[105] By not adopting such a broad concept of OSPs and making this provision facultative, ACTA succeeds in avoiding conflict with some domestic laws, such as the aforementioned E.U. law. However, lacking any concept of OSP creates legal uncertainty to the extent that implementing this recommendation may not help in harmonizing international enforcement, keeping in mind the differences between the DMCA approach in U.S. law,[106] domestic laws drafted according to FTAs,[107] and the E.U. directives.

The ACTA provision on identifying subscribers has a broad scope. This provision applies not only to copyright and related rights enforcement but also to trademark enforcement. Furthermore, at odds with negotiators' initial suggestions, this provision does not apply only for piracy and counterfeiting, but also for the criminal and civil enforcement of IP rights in general.[108]

104. Council Directive 2006/24, *supra* note 64, art. 3.2.

105. In the July 1, 2010 draft of ACTA, it was possible to appreciate a disagreement between those countries that wanted to apply this section to "*the Internet*" (Mexico, Singapore, and the United States) and those that wanted to extend its scope to "*digital environment*" (the European Union and Switzerland), which are already the words used in the provisional title of the whole section. *See* ACTA Draft—July 1, 2010, *supra* note 17, art. 2.18.1.

106. *See* 17 U.S.C. § 512 (2006) (providing that a service providers are not liable for monetary, injunctive, or equitable relief if the transmission of copyright material was initiated by a person who is not the service provider).

107. This may be the case in Chile, which in May 2010 implemented a Free Trade Agreement with the United States by imposing an obligation to identify users on OSPs other than those that provide mere access. *See* Ley 17.336 sobre Propiedad Intelectual, [Intellectual Property Act], Ago. 8, 1970, as amended, DIARIO OFFICIAL, May 4, 2010 (Chile), arts. 85 L to 85 U.

108. ACTA Text—Dec. 3, 2010, *supra* note 9, art. 27, ¶ 4 (extending the scope of the provisions that identify users for any infringement so long as the rights

However, the former matter—whether the provision encouraging the identification of subscribers would apply only to copyright and related rights or also to other IP rights—was not settled until the last round of negotiations.[109] The title of the section referred to enforcement of IP rights, generally, and some countries seemed to be pushing for such a broad approach, but luckily that approach was rejected for the final text of ACTA.[110] For now, the controversy has been solved in favor of a scope for this provision that extends only to trademark, copyright and related rights.[111] In spite of lacking mandatory effects, this could still be problematic for the United States, since the DMCA limits its provisions to enforce copyright and related rights; therefore, full compliance with the recommended standard of ACTA would require the adoption of legislative measures.

In addition to the fact that the scope of the provision on identifying subscribers is broad, 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.[112] Although negotiating parties recognized some gradation among criminal conduct,[113] for the purpose of

holder files a legally sufficient claim for "trademark and copyrights or related rights infringement").

109. ACTA Draft—Oct. 2, 2010, *supra* note 10, art. 2.18.4.

110. Australia, Canada, Mexico, New Zealand, Singapore, and the United States supported a scope limited to trademark, copyright and related rights, while the European Union, Japan, and Switzerland a broader approach, which extends to all intellectual property rights. *See* ACTA Draft—July 1, 2010, *supra* note 17, art. 2.18.1.

111. *Compare* ACTA Text—Dec. 3, 2010, *supra* note 9, art. 27, ¶ 2 (applying only to infringement of copyright or related rights), *and id*. art 27, ¶ 4 (applying to both trademark and copyright or related rights), *with* ACTA Draft—Oct 2, 2010, *supra* note 10, arts. 2.18.2 & 2.18.4 (applying to infringement of *at least* trademark and copyright or related rights).

112. *See* ACTA Text—Dec. 3, 2010, *supra* note 9, art. 23 (criminalizing not only "willful trademark counterfeiting or copyright . . . piracy on a commercial scale," but also unauthorized filming of cinematographic works, and aiding and abetting in the above crimes). *But see id.* art. 27 (applying the provisions on identifying users to trademark or copyright or related rights infringements).

113. *See, e.g.*, ACTA Draft—July 1, 2010, *supra* note 17, art. 2.14.1 (referring to criminal offenses in "cases of willful trademark counterfeiting or copyright or related rights piracy on a commercial scale"); *id.* art. 2.16.3 (mentioning

identifying users, ACTA does not make any distinction and seems to apply to any infringing activity. Given the initial purpose of the agreement and the lack of consensus about what constitutes a criminal offense, ACTA has had to introduce some restrictions in the application of the provisions on identifying users—for example, by limiting them to criminal actions concerning piracy.[114]

The provision about the identification of subscribers in ACTA applies not only to criminal enforcement, but also to civil enforcement.[115] Neither the provisions that encourage granting 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, exclude the provision on identifying Internet users from civil enforcement. This could be troublesome, as most countries require OSPs to retain traffic data for purposes of criminal prosecution, especially in the cases of so-called cybercrime,[116] but do not apply such data retention 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 IP rights that, after all, according to the TRIPS Agreement, are private rights.

In the case of the E.U., for example, the Data Retention Directive requires providers to process subscribers' personal data for the purpose of investigation, detection, and prosecution of serious crime.[117] However, according to the decision of the European Court of Justice in the case *Productores de Música de España (Promusicae) v. Telefónica de España SAU*, while Community law does not set forth a specific obligation upon E.U. members to

"indictable offenses" and "serious offenses"); *id.* art. 2.17 (referring to "cases of significant public interest"); *id.* art. 2.X (border measures - *de minimis* provision) (permitting an exception to border measures in case of *de minimis* infringement, which is not the case for granting access to personal data related to a supposed infringer).

114. ACTA Text—Dec. 3, 2010, *supra* note 9, art. 5 (k) (providing a concept of pirated copyright goods, but one that is still considerably broad and would require some changes in order to rationalize the scope of the criminal enforcement provisions).

115. *Id.* art. 27, ¶ 4.

116. *See, e.g.*, Convention on Cybercrime, *supra* note 85, art. 14, ¶ 2.

117. Council Directive 2006/24, *supra* note 64, art. 1.

guarantee access to Internet users' personal data for copyright holders in civil enforcement actions, Community law does allow the adoption of this kind of measure in domestic law.[118] In sum, full compliance with the encouraged terms of ACTA would require E.U. members to adopt domestic laws that oblige providers to identify subscribers for purposes of civil enforcement, even when it is not mandatory under Community law.

ACTA encourages the adoption of procedures granting access to the personal information of subscribers held by OSPs in order to facilitate IP enforcement. However, keeping in mind the initial purposes of ACTA, this article recommends an express limitation on the scope of such access to information, for example, by permitting that access in criminal cases involving copyright piracy and prohibiting that access in civil enforcement actions.

D. ACTA OMITS SPECIFIC SAFEGUARDS UNDER THE RIGHT TO PERSONAL DATA PROTECTION TO ENCOURAGE ACCESS TO PERSONAL INFORMATION OF INTERNET USERS.

While ACTA encourages granting access to Internet users' personal information for purposes of IP enforcement, during most of the negotiations, ACTA failed to include any measure to protect the rights of those concerned about an abusive use of that access mechanism. On the contrary, the July 1, 2010 ACTA draft seems to privilege expeditious access to data, without mentioning either substantive or procedural safeguards.[119] The absence of consideration for the rights to privacy and protection of personal data led to E.U. authorities calling attention to the matter, which presumably led to the inclusion of some flexibility in the latest version of ACTA.[120]

Besides the non-mandatory nature of the provision granting access

118. Case C-275/06, Productores de Música de España (Promusicae) v. Telefónica de España SAU, 2008 E.C.R. I-00271; *see* Ramón Casas Vallés, *Pursuing the P2P Pirates: Balancing Copyright and Privacy Rights*, WIPO MAGAZINE (English version), Apr. 2008, at 10-11 (interpreting *Promusicae* as holding that national legislatures can mandate access providers to disclose connection and traffic data; however, the legislatures' authority is limited by the fundamental rights under the Community legal order).

119. ACTA Draft—July 1, 2010, *supra* note 17, art. 2.18, ¶ 3.

120. *E.g.*, *Data Protection Supervisor Opinions*, *supra* note 66, ¶ 4; Letter from WP29, *supra* note 68.

to personal information of Internet users, the latest ACTA draft seems to have included at least three flexible provisions intended to ameliorate the noxious effects of such access: (1) the clause on privacy and disclosure of information set forth among the initial provisions,[121] (2) the article on general obligations with respect to enforcement included in chapter two of the agreement,[122] and (3) the sentence related to the implementation of the provision regarding the identification of users.[123] The first does not apply directly to the mechanism for identifying Internet users, but to the disclosure of information between ACTA parties; this provision is analyzed later in the context of cross-border transfers of personal data.[124] The second two provisions seem directly relevant to mitigating the effects of the provisions on identifying users.

The section on general obligations with respect to enforcement makes several statements relevant for our purpose: "[Enforcement] procedures shall be applied in such a manner as . . . to provide for safeguards against their abuse.";[125] "Procedures . . . to implement the provisions of this Chapter shall be fair and equitable, and shall provide for the rights of all the participants subject to such procedures";[126] and, "In implementing . . . this Chapter, each Party shall take into account the need for proportionality between the seriousness of the infringement, the interests of third parties, and the applicable measures . . . . "[127] This set of provisions provides an interesting legal framework to balance IP enforcement with adequate protection for the rights to privacy and protection of personal data. For example, to prevent abuse, domestic law could require right holders to provide relevant information before receiving access to personal data of supposed infringers; protecting the rights of all the participants could justify judicial control on request and delivery of data; and, the application of the principle of proportionality could imply excluding de minimis infringement from the scope of the provisions on identifying users. Therefore, countries that accept the

121. ACTA Text—Dec. 3, 2010, *supra* note 9, art. 4.
122. *Id.* art. 6.
123. *Id.* art. 27, ¶ 4.
124. *Id.* art. 22; *see infra* Part II.G.
125. *Id.* art. 6, ¶ 1.
126. *Id.* art. 6, ¶ 2.
127. *Id.* art. 6, ¶ 3.

challenge of including provisions on identifying users into their domestic law, as is encouraged by ACTA, cannot only set forth such obligation for OSPs; those countries must adopt safeguards as well.

In addition to the general obligation on enforcement, ACTA establishes a third set of provisions that tries to balance IP enforcement and the rights to privacy and protection of personal data in the section that sets forth rules on procedures for identifying users. According to ACTA, "[t]hese procedures shall be implemented in a manner that . . . consistent with that Party's law, preserves fundamental principles such as freedom of expression, fair process, and privacy."[128] This provision makes clear that, in spite of its absence during most of the negotiation, negotiating parties realized that enforcing IP could conflict with other competing interests, including the right to privacy. Therefore, ACTA admits that some concessions should be made in favor of privacy, but it does not mean that privacy concerns (or any other "fundamental principles") will block the adoption of rules on the identification of users.

These flexible ACTA provisions allow countries to adopt measures that guarantee the protection of the right to privacy in balance with IP enforcement, at least to some extent. By applying criteria such as proportionality and prevention of abuse, countries that decide to implement the provisions regarding the identification of users, encouraged by ACTA, can mitigate the noxious effects of those procedures that undermine the protection of privacy. However, the language of these protective ACTA provisions is extremely general and requires adopting concrete measures in domestic law. In this sense, those general statements seem insufficient to protect privacy and personal data processing in the context of IP enforcement online. ACTA runs short of provisions setting forth specific safeguards. For example, there are no rules regarding the amount of time OSPs should keep subscribers' personal data, procedures that properly guarantee the rights of concerned subscribers, or even which data should be kept.[129] It has even been

128. *Id.* art. 27, ¶ 4. Similar provisions are also available in other articles of ACTA on enforcement of intellectual property rights in the digital environment. *See id.* art. 27, ¶ 2 (covering the scope of enforcement procedures in civil cases); *id.* art. 27, ¶ 3 (promoting business cooperation).

129. Some of those safeguards (and useful boundaries) are typically included in other international instruments and E.U. law. *See, e.g.*, Convention on Cybercrime,

noted by E.U. authorities that ACTA's failure to specify any temporal limitation for the processing of personal data by OSPs could lead to a conflict with E.U. law.[130]

The absence of appropriate safeguards is contrary to the high standards of protection adopted by the E.U., and even the minimal formal requirements provided by the DMCA in the United States.[131] In the E.U., 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.[132] 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.[133] In the United States, even the most expeditious procedure for identifying an alleged infringer, provided by the DMCA, has some minimal required showings and mandates the filing of certain documents.[134] Even these minimal concrete safeguards are absent in ACTA.

ACTA succeeded in including some general safeguards for the right to privacy and protection of personal data, but, naturally, the actual efficacy of these general safeguards will be unclear until they

supra note 85, arts. 15-16; Council Directive 2006/24, *supra* note 64, arts. 5-7.

130. *See Data Protection Supervisor Opinions*, *supra* note 66, ¶ 80 (specifying that the duration of data retention shall be proportional to the recipient's purpose for retaining the data); *see also* Council Directive 2006/24, *supra* note 64, art. 6 (specifying that data shall be retained for no less than six months but no more than two years).

131. *See* 17 U.S.C. § 512(h) (2006) (requiring a copyright owner to request that the clerk of any U.S. District Court issue a subpoena to a service provider to determine the identity of an alleged infringer).

132. *See Productores de Música de España*, 2008 E.C.R. ¶ 70 (holding that E.U. member states are not required to mandate communication of personal data to ensure civil copyright enforcement; however, if a member states chooses to do so, it must ensure that interpretations of the mandate would not conflict with fundamental rights).

133. *See id.*

134. 17 U.S.C. § 512(h). Copyright holders may "request the clerk of any United States district court to issue a subpoena to [an ISP] for identification of an alleged infringer." *Id.* § 512(h)(1). This request must include a sworn declaration that the information is sought solely for the purpose of protecting copyright. Kao, *supra* note 101, at 410; *see* Julie E. Cohen, David E. Sorkin & Peter P. Swire, *Copyright & Privacy – Through the Privacy Lens*, 4 J. MARSHALL REV. INTELL. PROP. L. 273, 278 (2005) (arguing that the relevant DMCA's provisions are excessively permissive and seriously threaten privacy).

are applied. Regardless, the absence of *specific* safeguards in the agreement not only jeopardizes the protection of the right to privacy, but fails to advance legal harmonization among ACTA members. This could become a serious problem, particularly for those countries lacking adequate technical assistance and/or suffering from political pressure to turn over information about alleged infringers.

E. ACTA PROVIDES LEGAL SUPPORT FOR IMPLEMENTING THE POLEMICAL THREE STRIKES POLICY BY REQUIRING THE PROMOTION OF COOPERATIVE EFFORTS WITHIN THE BUSINESS COMMUNITY

The three strikes policy, also known as "graduated response," is a domestic legal mechanism allowing the disconnection of a supposed infringing Internet user for a given period of time, after the user has received warnings about, and failed to cease copyright infringement occurring via his Internet account.[135] At this time, only a handful of countries have passed laws adopting three strikes provisions, including France,[136] South Korea,[137] Taiwan,[138] the United Kingdom,[139] and New Zealand.[140]

135. *Three Strikes/Graduated Response*, CTR. FOR DEMOCRACY & TECH., http://www.cdt.org/issue/3-strikes-graduated-response (last visited Mar. 1, 2011).

136. Loi 2009-669 du 12 juin 2009 favorisant la diffusion et la protection de la creation sur internet [Law 2009-669 of 12 June 2009 on promoting the distribution and protection of creative works on the internet], JOURNAL OFFICIEL DE LA RÉPUBLIQUE FRANÇAISE [J.O.] [OFFICIAL GAZETTE OF FRANCE], June 13, 2009, p. 9666.

137. *See* Ju-jak-kwon-bup [Copyright Law], Act No. 3916, Dec. 30, 1989, *amended by* Act No. No. 9625, April 22, 2009, arts. 133-2 to 133-3 (S. Kor.), *available at* http://www.wipo.int/wipolex/en/text.jsp?file_id=190145 (authorizing the Minister of Culture, Sports, and Tourism to order ISPs to suspend for up to six months the accounts of those users who have been warned three times for transmitted illegal reproductions).

138. Copyright Act art. 90 *quinquies* (Taiwan) (modified May 2009), *available at* http://www.wipo.int/wipolex/en/text.jsp?file_id=187795 (providing that the service provider shall terminate the subscriber's service after three repeated infringements).

139. *See* Digital Economy Act, 2010, c. 24 § 9, 124G (U.K.) (describing that the service provider shall limit the speed or material available to the subscriber or simply suspend his service entirely).

140. 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. *See* Copyright (New Technologies Amendment Act 2008, First Schedule, cl 92A

The French three strikes law was introduced by President Nicolas Sarkozy's government, and probably best illustrates how polemical this policy can be.[141] The bill generated serious concerns for the French data protection authority over the protection of Internet users' personal data.[142] Once adopted by the legislature, the law was declared unconstitutional by the Constitutional Council because it infringed on the right to due process of law by allowing an administrative authority to impose sanctions,[143] by-passing the presumption of innocence by requiring the subscriber to prove he has not committed an infringement.[144] It also infringes on the right of free speech because "[i]n the current state of [affairs] . . . the participation in democracy and the expression of ideas and opinions [includes the] freedom to access [to those Internet] services."[145] Eventually, the unconstitutionality was remedied by the French Parliament, which empowered courts to disconnect Internet users.[146] Only after one year in force did the French authority start issuing warnings of infringement,[147] and to-date no one has been disconnected.[148] As

(N.Z.).

141. *E.g.*, *French Reject Internet Privacy Law*, B.B.C. NEWS (Apr. 9, 2009), http://news.bbc.co.uk/2/hi/7992262.stm.

142. *La Loi Antipiratage: le Gouvernement Critiqué par la CNIL*, LA TRIBUNE (Fr.), Nov. 3, 2008.

143. Conseil Constitutionnel [CC] [Constitutional Council], decision no. 2009-580DC, June 10, 2009, ¶¶ 16, 39 (Fr.).

144. *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, must prove his/her innocence notwithstanding any technical limitations. For example, the British Digital Economy Act set forth disconnection of users, euphemistically called technical measures, which may be adopted by Internet service providers; users can appeal the measure, but the *onus probandi* is on the user's shoulders. *See* Digital Economy Act § 124K. Thus, users are presumed guilty.

145. *Id.* ¶ 12.

146. Loi 498 du 24 juin 2009 relatif à la protection pénale de la propriété littéraire et artistique sur internet [Law 498 of June 24, 2009 relating to the criminal protection of literary and artistic property on the Internet] JOURNAL OFFICIEL DE LA REPUBLIQUE FRANÇAISE [J.O.] [OFFICIAL GAZETTE OF FRANCE], Oct. 29, 2009, p. 18290.

147. *See First warning letters sent by French ISPs under the Three Strikes System*, EUR. DIGITAL RTS. (Oct. 6, 2010), http://www.edri.org/edrigram/number8.19/first-email-three-strikes-france.

148. *See Francia inicia la segunda fase de avisos a los internautas que descargan sin permiso*, EL MUNDO (Spain) (Jan. 12, 2011), http://www.elmundo.es/elmundo/2011/01/12/navegante/1294839153.html. (reporting that the

Jérémie Zimmermann, the spokesperson of *La Quadrature du Net*, a French advocacy group that promotes rights and freedoms on the Internet, said it seems that the law has created a "big tax-sponsored spam machine."[149]

The French three strikes law also had an effect at the Community level. 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.[150] The conflict eventually was solved by adopting an amendment, resisted by Sarkozy's government, which requires that "[m]easures taken by Member States 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."[151]

Returning to the subject of ACTA, the first leaked versions included an explicit mention of the three strikes law in their footnotes, presented an example of a policy addressing the unauthorized storage or transmission of materials protected by copyright or related rights.[152] The content of that footnote was deleted in the official release of ACTA,[153] but ACTA retained the provisions that formed the basis for the three strikes policy, requiring

HADOPI is just working on a second round of warnings).

149. *Hadopi is dead: "three strikes" buried by highest court,* LA QUADRATURE (Fr.) (Jun. 10, 2009), http://www.laquadrature.net/fr/hadopi-is-dead-three-strikes-killed-by-highest-court.

150. *See* Leigh Phillips, *France Passes 'Three Strikes' Piracy Law*, BLOOMBERG BUSINESSWEEK (May 14, 2009, 1:43 PM), http://www.businessweek.com/globalbiz/content/may2009/gb20090514_391445.htm (noting that the French legislation was passed despite a European Parliament ruling that governments could not disconnect internet access without first receiving a court order).

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

152. *See* ACTA Draft—Jan. 18, 2010, *supra* note 16, art. 2.17.3 n.29 ("[A]n example of such a policy is providing for the termination in appropriate circumstances of subscriptions and/or accounts on the service provider's system or network of repeat infringers."); *see also* EUROPEAN UNION DIRECTORATE-GENERAL FOR TRADE, ACTA NEGOTIATIONS Ref. 588/09, (Sept. 30, 2009).

153. ACTA Draft—Apr. 21, 2010, *supra* note 14, n.58 (noting, instead, that at least one delegation proposed to include language in that footnote to provide greater certainty that their existing national law complies with the proposed article of ACTA).

that an OSP satisfy certain requirements to enjoy limited liability for online infringements.[154]

In addition to human rights concerns, disconnecting Internet users, as previous drafts of ACTA suggested, could be especially cumbersome for countries that already have recognized the rights to Internet access and/or to broadband.[155] But it is not just the sanction of the disconnection itself that causes concern, but also the lack of substantive and procedural safeguards for supposed infringers.[156] For example, previous drafts of ACTA did not impose a general monitoring requirement on OSPs,[157] but the implementation of a three strikes provision would necessarily require some processing of personal data without authorization from the user. Again, ACTA drafts failed to provide a minimum legal framework for such data processing.

The European authorities on data protection analyzed the ACTA provisions on three strikes and their negative effects on the right to privacy. According to the Supervisor and the WP29, the text of ACTA at the very least encouraged the implementation of the controversial three strikes policy.[158] 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 E.U. law.[159]

Presumably because of the criticism against the three strikes provision included in the drafts of ACTA and the disagreement among negotiating parties around the limitation of liability for OSPs in cases of online infringements, the last version of ACTA does not include either of them.[160] However, it does not mean that the three

154. *Id.* art. 2.18.3.

155. *See, e.g.*, Communications Market Act, amended in September 2009, §60 d (331/2009) (Fin.) (recognizing the access to broadband service as a legal right through a universal service obligation); Corte Suprema de Justicia [C.S.J.] [Supreme Court], Sala. Const. Julio 30, 2010, decision no. 2010012790, ¶ IV (Costa Rica) (recognizing an autonomous right to access to the Internet through the interfaces chosen by consumers and users).

156. *See supra* Part II.D.

157. ACTA Draft—July 1, 2010, *supra* note 17, art. 2.18.3.

158. *See Data Protection Supervisor Opinions, supra* note 66, ¶ 15; Letter from WP29, *supra* note 68.

159. Letter from WP29, *supra* note 68.

160. ACTA Text—Dec. 3, 2010, *supra* note 9, art. 27.

strikes policy has been successfully counteracted in ACTA; in fact, it still survives under the requirement to promote cooperative efforts within the business community.[161] Such cooperative efforts could reasonably take the form of a privately implemented three strikes regime, because OSPs may feel forced to implement disconnection of users to avoid litigation with right holders, particularly in those countries that lack adequate protection for Internet users.

During the negotiations of ACTA, one article required parties to promote the development of mutually supportive relationships between OSPs and rights holders to deal with IP infringement online, and encouraged the establishment of guidelines.[162] In the last text of ACTA, that article has become broader in scope, by imposing on parties the obligation to promote cooperative efforts within the business community to effectively address infringement—obligations that apply to trademark, copyright, and related rights infringements.[163] On this point, it is important to note here that the self-regulatory approach has been used in some countries, such as the United Kingdom[164] and Ireland,[165] to promote the adoption of three strikes policies by the OSPs. Under the pressure from copyright holders and with the implicit agreement of governments, OSPs have modified their contracts with subscribers to include clauses that legitimize the disconnection of users for supposed copyright infringements.[166] This raises the issue of limiting the waiver of fundamental rights through contractual clauses, which is beyond the purpose of this article.

161. *Id.* art. 27, ¶ 3.

162. ACTA Draft—July 1, 2010, *supra* note 17, art. 2.18.3 *quater*.

163. ACTA Text—Dec. 3, 2010, *supra* note 9, art. 27, ¶ 3.

164. *See* Christian L. Castle & Amy E. Mitchell, *What's Wrong With ISP Music Licensing?*, 26 ENT. & SPORTS L. 4, 6 (2008) (referencing a July 24, 2008 "Memorandum of Understanding" signed between the principal U.K. record label trade association and the U.K.'s six largest service providers); *see also* Eleanor Dallaway, *Music Piracy Born Out of a 'Something for Nothing' Society*, INFOSECURITY, Apr. 2008, at 16, 17-20.

165. *See* KARLIN LILLINGTON, *Putting Up Barriers to a Free and Open Internet*, IRISH TIMES, Apr. 16, 2010, http://www.irishtimes.com/newspaper/finance/2010/0416/1224268442542.html (noting that self-regulation began in the area of child pornography, but has since expanded to the problem of cybercrime, and reporting the interest of the Irish government to implement a three strikes policy).

166. *Cf. id.* (recounting discussions between the government and OSPs on also introducing internet filtering technology for their subscribers).

Promoting cooperation and self-regulation seems adequate to deal with the continuous changes and challenges of the technological environment, and without the usual delay of legal solutions. However, it should not become the source of practices that undermine the rights of third parties, particularly the Internet end-users. Fortunately, the final text of ACTA takes advantage of previous experiences and includes two sets of safeguards, albeit minimal ones, against possible excesses of the so-called cooperative efforts. The first set is the previously mentioned article on general obligations with respect to enforcement, according to which the implementation of procedures shall avoid their abuse, protect the rights of all the participants, and take into account the need for proportionality.[167] The second set of safeguards appears immediately after the obligation on cooperative efforts. According to ACTA, parties shall promote that cooperation "while . . . consistent with each Party's law, preserving fundamental principles such as freedom of expression, fair process, and privacy."[168] These safeguards, appropriately included in the last version of ACTA, should help in mitigating the use of the obligation to promote cooperative efforts within the business community as a pretext to introduce a three strikes policy, and undermine the rights to privacy and protection of personal data.

However, given the excesses of contractual measures tolerated in some legal regimes, safeguards adopted under ACTA could become insufficient in some cases. For that reason, and given the intrinsic punitive nature of the three strikes policy—actual modern day ostracism, ACTA mentions that freedom of expression, fair process, and privacy could be not enough. In other words, ACTA has had to defer to the basic principles of criminal and human rights laws, 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.

In sum, the final version of ACTA does not include explicit references to either the three strikes policy or the requirement for an

167. *See* ACTA Text—Dec. 3, 2010, *supra* note 9, art. 6 (requiring states parties to consider the seriousness of any infringement against the interests of third parties in addition to applicable measures, remedies, and penalties).

168. *Id.* art. 27, ¶ 3.

OSP to qualify for the limitation of liability of IP infringements online; however, ACTA requires that parties promote cooperative efforts within the business community, which could lead to the implementation of a three strikes policy. For this case, ACTA has adopted some reasonable safeguards in order to balance IP enforcement with the rights to privacy and protection of personal data. However, those safeguards may not be enough and, given the punitive nature of the three strikes policy, ACTA has had to include stronger preventions.

F. ACTA EMPHASIZES THE PROTECTION OF EFFECTIVE TECHNOLOGICAL MEASURES, BUT DOES NOT AFFORD PROTECTION FOR THE PRIVACY AND PERSONAL DATA OF USERS AFFECTED BY SUCH MEASURES

The ACTA negotiators have provided a significant boost in the legal protection of effective technological measures, beyond the standard adopted in the WIPO Internet Treaties.[169] Before the official public release of ACTA, it required not only adequate legal protection and effective legal remedies, but also civil remedies or criminal penalties,[170] independent of any infringement of copyright or related rights.[171] Both mentioned requirements were excesses that do not appear in the last version of ACTA.[172] But, similar to the DMCA, ACTA still requires adopting anti-circumventing and anti-trafficking provisions, the latter of which implies serious difficulties in making real the possible safeguards that a country "may" adopt in favor of the users whose rights are protected through certain exceptions and limitations to copyright and related rights.[173] Unfortunately, unlike the DMCA and the FTAs signed by the United States with several countries, ACTA does not provide even a minimum list of those exceptions.

Analyzing the provisions about the legal protection of the effective

169. *See* World Intellectual Property Organization Copyright Treaty, *supra* note 33, art. 11 (obligating contracting parties to provide "adequate" and "effective" legal remedies against copyright infringers); World Intellectual Property Organization Performances and Phonograms Treaty, *supra* note 33, art. 18.

170. ACTA Draft—Jan. 18, 2010, *supra* note 16, art. 2.18.4.

171. ACTA Draft—July 1, 2010, *supra* note 17, art. 2.18.5.

172. ACTA Text—Dec. 3, 2010, *supra* note 9, art. 27, ¶ 5.

173. *Id.* art. 27, ¶ 6.

technological measures is beyond the purpose of this paper. However, besides the copyright limitations and exceptions allowed by ACTA, it fails to include any specific limitation that guarantees the adequate protection of the rights to privacy and the protection of personal data. It is still possible to apply the safeguards adopted in the general obligations to enforcement, particularly the one that requires parties to take into account the need for proportionality,[174] but it is not clear to which extent these safeguards will be enough to counteract the risk to the rights to privacy and protection of personal data. On the other hand, it is clear that including a provision that provides safeguards for those rights is necessary insofar as technological measures process personal data of people who use or access protected works.

G. ACTA OMITS PROVISIONS TO SAFEGUARD PROPERLY THE PROTECTION OF PERSONAL DATA IN CROSS-BORDER TRANSFERS OF SUCH DATA

Complying with or enforcing IP rules requires, to some extent, exchanging personal information between parties, such as data about copyright holders and supposed infringers. This is especially true in the case of online infringements; overcoming the limitations of territorially-based domestic laws demands a global answer, which calls for international cooperation in the enforcement of the law. In the case of ACTA, countries that adhere to the agreement shall share relevant information and shall adopt some enforcement practices that require processing information, including, potentially, personal data.[175] Therefore, ACTA requires cross-border transfers of personal data[176] and, as a result, ACTA has had to deal with provisions safeguarding some level of protection for the personal information that is transferred from one country to another.[177]

Several countries already have personal data protection laws, which balance the protection of people's privacy with the free flow of information. However, as it was understood early on by the

174. *See id.* art. 6, ¶ 3.

175. *Id.* art. 34.

176. *Id.* art. 29, ¶ 1(b) (permitting parties to share information, acquired through border enforcement, with other parties).

177. *Id.* art. 33, ¶ 3 (cautioning that the implementation of international cooperation must be consistent with relevant international agreements).

European countries, the very purpose of having strong domestic protection could be eroded if personal data is transferred to countries with lesser (or no) protection; cross-border transfers of personal data to places where there is not an adequate level of protection circumvents the objective of data privacy laws.[178] Therefore, for those countries it is necessary to adopt some limitations to those international transfers of data.

It is not by chance that the Supervisor raised concerns over the lack of provisions on cross-border transfers of personal data in the previous drafts of ACTA. There have been some attempts to regulate those transfers in international fora through legal harmonization, but their success, if there was any, has been limited.[179] But, this has not been the case for the E.U. Since the early 1980s, the E.U. has built an increasing level of protection for personal data in its internal market through the adoption of specific normative measures on the matter.[180] Basically, this legal framework assumes an "equivalent" level of protection among the E.U. members, which cannot block transfers in the internal market,[181] and requires an "adequate" level of protection in third countries before data can be transferred to them.[182] Therefore, apart from some limited exceptions,[183] transferring personal data to third countries that do not provide adequate levels of protection, which is the case for all the countries involved in the ACTA negotiations,[184] is banned.

178. *See Data Protection Supervisor Opinions*, *supra* note 66, ¶ 76 (warning that if transfer of personal data to third parties is necessary, specific data protection guarantees should accompany the transfer to ensure proper data protection in the third country).

179. *See supra* note 75-78 and accompanying text.

180. *See e.g.*, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Jan. 28, 1981, E.T.S. No. 108 (attempting for first time the harmonization of personal data protection law among countries of the European community); *see also supra* notes 60, 63-64.

181. Council Directive 95/46, *supra* note 60, ¶¶ 8-9.

182. *Id.* ¶¶ 56-57, 59-60; *id.* art. 25.

183. *Id.* art. 26 (banning the transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection except in the indicated cases).

184. *Commission Decisions on the Adequacy of the Protection of Personal Data in Third Countries*, EUR. COMMISSION, http://ec.europa.eu/justice/policies/privacy/thridcountries/index_en.htm (last visited Mar. 1, 2011) (listing countries that provide adequate level of protection, according to E.U. authorities: Andorra, Argentina, Faeroe Islands, Guernsey, Isla de Man, Israel, Jersey, and Switzerland,

ACTA negotiators, for most of the negotiations, avoided acknowledging the fact that a satisfactory solution for transfers of personal data is required for IP 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 main European authorities—the Commission that negotiated ACTA and the Parliament that has to approve negotiations—have been the result of the more sympathetic engagement of the latter as opposed to the former in protecting the right to privacy. First, the European Parliament rejected the agreement between the European Commission and the United States to transfer the personal data of air passengers, an issue that was eventually resolved through the European Court of Justice.[185] Second, the Parliament adopted a provision against the three strikes policy in the Telecom Package against the Commission's desires.[186] These facts show that privacy is a serious issue for European authorities, which ACTA negotiators did not weigh properly.

Presumably because of E.U. concerns, during the last rounds of negotiations, ACTA included some provisions dealing with the disclosure of information from one party to another. According to an initial provision, nothing in ACTA "shall require any Party to disclose: (a) information the disclosure of which would be contrary to its law or its international agreements, including laws protecting right of privacy, [or] (b) confidential information, the disclosure of which would impede law enforcement or otherwise be contrary to the public interest."[187] In other words, ACTA allows parties to preserve limitations on the disclosure of information to other countries already available in their domestic laws or international agreements. This should help in preventing conflict between ACTA obligations to provide data from one country to another and national laws that ban

but noting that there has been some authorized transfer of data in limited cases to other countries, such as Canada and the United States).

185. *See* Cases C-318/04 & C-317/04, Parliament v. Comm'n, 2004 E.C.R. I-4721, ¶¶ 67-70.

186. *See* Council Directive 2009/140, *supra* note 151, art. 1(1)(b)(3a).

187. ACTA Text—Dec. 3, 2010, *supra* note 9, art. 4, ¶¶ 1(a)-(b). There is a third clause in this article, which also sets forth an exception to the disclosure of information, but it deals with confidential information of particular enterprises, not personal data. *Id.* art. 4, ¶ 1(c).

cross-border transfers of personal data to third countries lacking a given level of protection.

In addition, ACTA sets forth a limitation of the use of transferred data by a receiving party. According to a clause introduced just in the penultimate round of negotiation, a party that has received information "shall . . . refrain from disclosing or using the information for a purpose other than that for which the information was provided, except with the prior consent of the Party providing the information."[188] This clause intends to neutralize the risk of a country using ACTA provisions as a mere pretense to access data from another country.

Unfortunately both aforementioned provisions are insufficient to guarantee an adequate level of protection for personal data otherwise required in some countries.[189] Unlike E.U. law, the ACTA provision on disclosure curiously refers only to disclosing information, but does not seem to apply to transfers and, more broadly, to processing personal data as a whole. Also, the second provision, which requires a receiving party to refrain from using the data for other purposes, sets forth some limitations on its scope. First, it applies only when a party has provided "written" information; and, second, the receiving party shall refrain from disclosing or using the date, but "subject to its domestic law and practice."[190] These two conditions significantly undermine the protection of personal information in a potential receiving country.

However, the main problem in regulating the cross-border transfers of data in ACTA is that it limits its concern to the parties' disclosure and use of the information. ACTA provisions on sharing and disclosing information need a broader approach to cross-border transfers of data. ACTA has had to provide an adequate level of protection by adopting substantive provisions related to the applicable rules and the means for ensuring their effective application. However, an adequate level of protection requires the existence of provisions that guarantee rights to data subjects, impose obligations on data controllers, set principles applicable to data processing, allocate responsibility in case of violations, and provide

188. *Id.* art. 4, ¶ 2.
189. *See supra* notes 184-85.
190. ACTA Text—Dec. 3, 2010, *supra* note 9, art. 4, ¶ 2.

real enforcement. Therefore, especially under E.U. law, ACTA fails in providing enough protection to permit transfers of personal data among the negotiating parties.

CONCLUSIONS AND REMARKS

Authorizing any intrusion into the privacy and personal data protection of Internet users under the guise of IP enforcement is disproportionate, and allows an excessive misuse and abuse of disclosed information. This jeopardizes the right to privacy—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 perpetrator of serious infringement, is likewise excessive. After the public disclosure of ACTA negotiations, negotiators tried to balance the competing interests in this dilemma: the rights to privacy and the protection of personal data with IP enforcement.

ACTA has grown to exceed the stated purpose of the treaty—fighting counterfeiting and piracy—and instead includes provisions intended to enforce the law against citizens, which are serious and unprecedented concessions.[191] In spite of the later inclusion of some safeguards, ACTA still omits appropriate substantive and procedural safeguards for the right to privacy of Internet users. Instead of limiting the access to personal data for serious crimes, ACTA encourages granting access to personal information beyond domestic laws in force. Even other international instruments that have been seriously criticized for being intrusive on privacy, such as the Convention on Cybercrime, seem more protective on the matter.[192]

In addition, ACTA provides legal support for implementing the polemical three strikes policy, a measure that raises several concerns from a human rights perspective, by promoting cooperation between right holders and OSPs. 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 problem arises in the harmonization between ACTA

191. *See supra* note 7 and accompanying text.
192. *See supra* note 116.

provisions allowing transfers of personal information among the parties and E.U. requirements for cross-border transfers of personal data. Currently, none of the negotiating parties satisfy the E.U.'s "adequate" level of protection to allow transfers of personal data;[193] therefore, national and communitarian authorities on data protection in the E.U. could block any transfer of such data for IP enforcement. Later negotiations of ACTA tried to handle this issue by including some safeguards on disclosing and using data transferred from one country to another; however, those provisions are not enough and their insufficiency to deal with cross-border transfers of personal data could become a serious obstacle in the adoption of ACTA by the European Parliament.[194]

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—to provide an international framework for harmonizing the fight against counterfeiting and piracy. For example, ACTA attempts to deal with any use of a copyrighted work in the digital environment, without providing a common understanding on essential issues for Internet regulation, such as limitations or the exceptions to IP rights and the exhaustion of those rights.[195] In fact, because of the lack of consensus, negotiators gave up on the most relevant provision to dealing with online IP infringements—the one related to the limitation of liability for OSPs.[196]

IP rights are essentially private rights and should rarely override the rights to privacy and personal data protection, which have an intrinsic social value, particularly in democratic societies. Unfortunately, ACTA makes mistakes when it exceeds its own

193. *See supra* notes 182-185 and accompanying text.

194. *See supra* notes 185-186 and accompanying text.

195. ACTA enforces intellectual property on digital environments. However, it does not advance the harmonization of copyright exceptions and limitations; for example, it does not clarify the status of transitory copies, which are essential for the very functioning of the Internet and are still illegal under some domestic laws. ACTA also omits a common understanding about exhaustion of rights because providing works online from one country to another may infringe the domestic law of those countries that award exclusive import rights to right holders and, therefore, require authorization to made available the work in different countries at once.

196. *See supra* note 37.

purpose by unnecessarily diminishing the right to privacy and the right to protection of personal data. It ultimately promotes IP enforcement not against smugglers and pirates, but against ordinary citizens.