"MAKE MONEY WITHOUT DOING EVIL?" CAUGHT BETWEEN AUTHORITARIAN REGULATIONS IN EMERGING MARKETS AND A GLOBAL LAW OF HUMAN RIGHTS, U.S. ICTS FACE A TWOFOLD QUANDARY

By Brian R. Israel

In 2004, Yahoo!'s Hong Kong subsidiary received a request from the Beijing State Security Bureau for information about a Yahoo! email account registration, login times, and associated IP addresses.[1] The request cited the account-holder's "illegal provision of state secrets to foreign entities."[2] Yahoo! Hong Kong complied with the request and furnished information leading to the identification of a Chinese journalist named Shi Tao. On the U.S.-based Internet site "Democracy Forum," Shi Tao had described a Chinese government warning to journalists to avoid making anti-government statements and to report any contact with human rights activists.[3]

Enabled by the information from Yahoo!, the Chinese government kidnapped Shi Tao and detained him for weeks without charge before sentencing him to ten years in prison, where he allegedly endures torture.[4] With the help of human rights organizations, the families of Shi Tao and Wang Xiaoning (another dissident persecuted after Yahoo! provided Chinese authorities with identifying information) sued Yahoo! in U.S. federal court under the Alien Tort Claims Act,[5] claiming that Yahoo! aided and

---

1. Beijing State Security Bureau, Notice of Evidence Collection, 2004 BJ State Sec. Ev. Coll. No. 02, *original and English available at* http://www.duihau.org/press/news070725_ShiTao.pdf.

2. Id.

3. Human Rights Watch, "Race to the Bottom:" Corporate Complicity in Chinese Internet Censorship, Volume 18, No. 8(C) (2006) p. 107.

4. *Yahoo! Inc.'s Provision of False Information to Congress, Hearing Before H. Comm. On Foreign Affairs*, 110th Cong. 7 (2007) (Representative Christopher Smith expressed his belief that "based on our best information, [Shi Tao] is being tortured").

5. As explained below, this statute confers federal jurisdiction for gross violations of international law. *See* discussion *infra* Section I.B.2.

abetted torture and arbitrary detention.[6] Following two contentious appearances before congressional committees, Yahoo! settled with the families of Shi Tao and Wang Xiaoning in February 2007.[7]

Shi Tao's fate is unfortunately not unique. Contrary to predictions that the Internet would energize progressive reform in authoritarian states,[8] such states have proven capable of controlling the Internet within their territories, restricting unfavorable information and persecuting so-called "cyber dissidents"—activists using the Internet as a platform for political dissent.[9] A telling symptom of this repressive control is that internet journalists now comprise the single largest group of imprisoned journalists worldwide.[10] Nowhere are more internet journalists imprisoned than in China, which maintains the world's most extensive and sophisticated system for internet censorship and surveillance.[11]

Nor is the entanglement of U.S. information and communication technology companies (ICTs) in such human rights abuses likely to subside. Leading U.S. ICTs such as Yahoo!, Microsoft, and Google have come to China, drawn by unparalleled opportunities in the world's largest Internet market.[12] These companies embrace identities that combine altruism with innovation;[13] indeed, Google's well-known corporate philosophy is to

---

6. Second Am. Compl., Xaioning et al v. Yahoo! Inc. et al, No. C07-02151 (N.D. Cal. Jul. 30, 2007) [hereinafter *Shi Tao complaint*] *available at* http://www.humanrightsusa.org/index.php?option=com_docman&task=doc_download&gid=68&Itemid=99999999.

7. Joint Stipulation of Dismissal, Xaioning et al v. Yahoo! Inc. et al, No. C07-02151 (N.D. Cal. Nov. 13, 2007).

8. *See, e.g.*, Nicholas D. Kristof, *Death by a Thousand Blogs*, N.Y. TIMES, May 24, 2005, at A21.

9. S*ee generally* Robert Faris and Nart Villeneuve, *Measuring Global Internet Filtering, in* ACCESS DENIED: THE PRACTICE AND POLICY OF GLOBAL INTERNET FILTERING 5 (Ronald Deibert, John Palfrey, Rafal Rohozinski, Jonathan Zittrain, eds., 2008).

10. COMMITTEE TO PROTECT JOURNALISTS, CPJ 2008 PRISON CENSUS: ONLINE AND IN JAIL, 1 (2008), http://cpj.org/imprisoned/cpjs-2008-census-online-journalists-now-jailed-mor.php.

11. As of December 4, 2008, 24 of 28 journalists imprisoned in China were internet journalists. *Id.* at 2; *see also* Human Rights Watch, *supra* note 3, at 9.

12. The number of Internet users in China recently eclipsed the United States, making China the world's largest Internet market. David Barboza, *China Surpasses U.S. in Number of Internet Users*, N.Y. TIMES, Jul. 26, 2008, at C3.

13. *See, e.g.*, Letter from Jerry Yang, CEO of Yahoo! Inc., to Condoleezza Rice, U.S. Secretary of State (Feb. 21, 2008) *available at* http://www.bayareanewsgroup.com/multimedia/mn/news/yang_letter_022208.pdf; Microsoft Corporate Citizenship site, http://www.microsoft.com/about/corporatecitizenship/us/default.mspx (last visited Sept. 20, 2008).

"make money without doing evil."[14] The Chinese government and its policies have tested that ethos. Unable to consummate its control over the Internet in China without the cooperation of private ICTs, the Chinese government requires ICTs to actively filter Internet content deemed unfavorable and to hand over user-information.[15]

It seems uncontroversial that U.S. ICTs face a *moral* dilemma when asked to assist with censorship and persecution of political dissidents. This often unspoken assumption pervades news reports,[16] statements by nongovernmental organizations (NGOs),[17] and congressional hearings[18] on the issue. Less appreciated, or at least insufficiently articulated, is that operating in internet-restricting countries presents a profound *business* quandary for U.S. ICTs, threatening crucial assets. This business quandary is the result of conflicting standards to which ICTs are simultaneously subject: the local regulations of authoritarian states, and a global standard informed by international human rights norms and societal expectations in the companies' home markets.

This Note seeks to articulate the business quandary facing U.S. ICTs operating in countries that condition market access on cooperation with state-imposed censorship and political persecution. Part I delineates the components of what shall be termed the *global law* with which ICT conduct must conform separate and apart from the local laws of authoritarian states. It then identifies a spectrum of business consequences for noncompliance with the global law that transcend mere moral objection. For ex-

---

14. Google, *Corporate Information – Our Philosophy*, http://www.google.com/corporate/tenthings.html (last visited February 2, 2009).

15. In 2002, the Chinese Information Ministry reportedly required foreign ICTs to sign a "self-discipline pact" obligating them "not to produce or disseminate harmful texts or news likely to jeopardise national security and social stability, violate laws and regulations, or spread false news, superstitions and obscenities." The "self-discipline pact" further requires of ICTs "co-operation by sites in the fight against cybercrime and against the violation of intellectual property rights." Reporters Without Borders for Press Freedom, "Living Dangerously on the Net:" Censorship and surveillance of Internet Forums, May 12, 2003, http://www.rsf.org/print.php3?id_article=6793 (last visited Sept. 21, 2008).

16. *See, e.g.*, Nicholas D. Kristof, *China's Cyberdissidents and the Yahoos at Yahoo*, N.Y. TIMES, Feb. 19, 2006, § 4, at 13.

17. *See, e.g.*, Press Release, Human Rights Watch, China: Internet Companies Aid Censorship (Aug. 8, 2006), *available at* http://www.hrw.org/en/news/2006/08/08/china-internet-companies-aid-censorship.

18. See, e.g., The Internet In China: A Tool For Freedom or Suppression? Hearing Before H. Subcomm. On Africa, Global Human Rights, and International Operations, and H. Subcomm. Asia and the Pacific, H. Comm. On International Relations, 109th Cong. (2006).

ample, ICT conduct that leads to grave violations of international law—such as torture, extrajudicial killing, and prolonged arbitrary detention[19]—can lead to U.S. federal court actions under the Alien Tort Claims Act.[20] Part II examines recent responses to this quandary by the federal government, NGOs and ICTs. Most promising is the Global Network Initiative launched in October 2008, a comprehensive code of conduct and accountability mechanism that is the result of ongoing collaboration among ICTs, NGOs, academics, and investors. Although the problem cannot be completely overcome by nongovernment actors, the Global Network Initiative represents the best available opportunity for ICTs that wish to seize opportunities in emerging markets while adhering to their core values, avoiding litigation exposure, and safeguarding their brands and human capital.

I. THE BUSINESS QUANDARY

The business quandary can be summarized as follows. Competitive necessity drives ICT expansion into new markets, including repressive states that brutally suppress political dissent. Some such states require—by law or "voluntary" agreement—that ICTs assist the government by restricting Internet content and providing user-identifying information upon request. Companies are thus simultaneously subject to two conflicting laws: the local law and a *global law* comprising international human rights standards, company and industry codes of conduct, and the expectations of key stakeholders. Where, as in the Shi Tao case, a government requests identifying information that may lead to the persecution of a user, ICTs presently face a choice between strained ties with the host government or an Alien Torts Claim Act suit and public condemnation at home. Where the immediate human consequences of government demands are less dramatic—as is often the case with content filtering—the consequences are subtler, but the corrosive effects on brand and human capital may nonetheless impair competiveness in the long term.

A. Defining the Contours of the "Global Law"

Global law, as used here, means a standard of conduct independent of any national legal system backed by consequences for noncompliance.[21] Apart from local laws, the standard governing ICT involvement in states'

19. *See infra* Section I.B.2 (identifying the state action for which ICTs may be accessorily liable).

20. 28 U.S.C. § 1350 (2006).

21. The concept of a "global law" is inspired by Joe W. (Chip) Pitts III, *Business, Human Rights, & the Environment: The Role of the Lawyer in CSR & Ethical Globalization*, 26 BERKELEY J. INT'L L. 479, 488 (2008).

assertion of repressive control over the Internet is international human rights law. This body of treaties, customary international law and judicial decisions binds states in the first instance. As relevant here, it proscribes state-interference with expression, privacy, and physical persecution.[22] International human rights law becomes relevant to private ICTs when they *assist* state actions that violate human rights norms; for example, by filtering Internet content, intercepting electronic communications, and providing user-identifying information to state authorities.

Some measure of the state interference with privacy and expression is broadly accepted in even the most liberal democracies as necessary to secure vital public goods.[23] International human rights law demarcates the admittedly blurry line between governmental control of the Internet that is accepted, and that which carries adverse consequences for ICTs. ICT assistance with some state conduct on the wrong side of that line is actionable in U.S. courts.[24] In many instances the global law is enforced through non-legal means.[25]

Google, Yahoo! and Microsoft recently became more directly accountable for human rights norms through membership in the Global Network Initiative.[26] Through the Initiative they have voluntarily agreed to abide by a code of conduct that codifies international human rights law and to subject their operations to independent assessments of their compliance with these standards.[27] And for those ICTs not yet participating in the

---

22. *See, e.g.*, Articles 17 (privacy) and 19 (expression) of the International Covenant on Civil and Political Rights, Mar. 23, 1976, General Assembly Resolution 2200A(XXI) [hereinafter ICCPR]; RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW OF THE UNITED STATES § 702 (1987) (stating that torture and prolonged arbitrary detention constitute violations of international law).

23. JACK GOLDSMITH & TIM WU, WHO CONTROLS THE INTERNET? ILLUSIONS OF A BORDERLESS WORLD 65-86, 129-146 (Oxford Univ. Press 2006). In the United States, Internet restrictions necessary to protect intellectual property are widely accepted, such as those effected by the Digital Millennium Copyright Act, 35 U.S.C. § 512. Several western European states impose bans on hate speech and content deemed harmful to public morals. Laws in Britain, Germany and France require ICTs, upon notice, to take down child pornography, Nazi hate speech and illegal adoption sites, for example. Goldsmith & Wu at 73. *See also* Jonathan Zittrain and Benjamin Edelman, "Localized Google search result exclusions," http://cyber.law.harvard.edu/filtering/google/ (last visited October 12, 2008) (comparing search results on google.com to google.de and google.fr and finding fewer results available on the latter two).

24. *See* discussion of the Alien Tort Claims Act *infra* Section I.B.2.

25. *See infra* Section I.C.

26. *See infra* Section II.A.

27. Press Release, Global Network Initiative, Diverse Coalition Launches New Effort to Respond to Government Censorship and Threats to Privacy (Oct. 28, 2008), *available at* http://www.globalnetworkinitiative.org/newsandevents/Diverse_Coalition_

Global Network Initiative, international human rights law remains the standard against which NGOs measure ICT conduct.

B. Applicable International Human Rights Norms

Two categories of international human rights norms apply to ICT operations. Addressed first are those norms implicated when ICTs assist governments in Internet filtering and surveillance. Because the objective of this analysis is to delineate a global standard, it draws upon both international and regional human rights conventions and the jurisprudence of regional, national, and international tribunals. It matters little whether these instruments are "non-binding" because this law is more likely to be enforced in the so-called "court of public opinion" than in a judicial forum. What is most relevant is the convergence of norms and jurisprudence across continents. It is from this consensus that a global standard can be discerned.

Where ICT conduct leads to physical persecution by a state (limited here to torture, extrajudicial killing and prolonged arbitrary detention) a second set of human rights norms and consequences are implicated. Because victims of state persecution can directly assert this second category of norms in a judicial forum, Section I.B.2 will focus on sources cognizable in U.S. federal courts.

1. Human Rights Standards Relevant to Internet Filtering, Surveillance, and Provision of Personal Information.

Internet filtering, providing personal information, and intercepting or accessing electronic communications interfere with the freedom of expression and the right to privacy protected by international human rights law. Both rights are found, in substantially the same form, in the principal international human rights instruments, regional human rights conventions, and national constitutions.[28] The most globally ratified expression of these

---

Launches_New_Effort_To_Respond_to_Government_Censorship_and_Threats_to_Privacy.php (last visited Dec. 19, 2008).

28. Examples of international human rights instruments include Articles 17 (privacy) and 19 (expression) of the ICCPR, G.A. Res. 2200A (XXI), U.N. GAOR Supp. (No. 16), at 52, U.N. Doc A/6316 (Dec. 16, 1966) and Articles 12 (privacy) and 19 (expression) of the Universal Declaration of Human Rights, G.A. Res. 217A, at 71, U.N. GAOR, 3d Sess., 1st plen. mtg., U.N. Doc A/810 (Dec. 10, 1948). Examples of regional human rights instruments include Articles 8 (privacy) and 10 (expression) of the European Convention for the Protection of Human Rights and Fundamental Freedoms, Nov. 4, 1950, 213 U.N.T.S. 222; Articles 7-8 (privacy) and 11 (expression) of the Charter of Fundamental Rights of the European Union, Dec. 18, 2000, 2000/C 364/01; Article 9 (expression) of the African Charter on Human and Peoples' Rights, Oct. 21, 1986, OAU Doc. CAB/LEG/67/3, 22 I.L.M. 58; Articles IV (expression) and V (privacy) of the

rights is the International Covenant on Civil and Political Rights (ICCPR).[29] The freedom of expression is guaranteed by Article 19 of the ICCPR, which provides that everyone "shall have the right to hold opinions without interference,"[30] and that the right to freedom of expression "shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice."[31] The right to privacy is anchored in Article 17 of the Covenant, which protects against "arbitrary or unlawful interference with . . . privacy . . . or correspondence."[32]

The positive statements of rights in Articles 17 and 19 of the ICCPR only partially reveal the content of the rights to freedom of expression and privacy. Even more instructive are the circumstances under which derogation from these rights is permitted. Unlike the prohibition on torture,[33] for example, the rights to freedom of expression and privacy are not absolute. Article 19(3) of the ICCPR permits restrictions on the freedom of expression, where "provided by law and [] necessary . . . for the protection of national security or of public order . . . or of public health or morals."[34] These broad principles are given greater precision by the reports of international bodies such as the *Siracusa Principles*[35]—formulated by a high level conference of international law experts—and the General Comments

---

American Declaration of the Rights and Duties of Man, 1948, O.A.S. Res. XXX; Articles 11 (privacy) and 13 (expression) of the American Convention on Human Rights, Jul. 18, 1978, EA/ Ser.L.V/II.82 doc. 6 rev. 1. The First Amendment to the Constitution of the United States guarantees the freedom of expression. U.S. CONST. amend. I; *Even the Constitution of China* provides, "[c]itizens of the People's Republic of China enjoy freedom of speech, of the press, of assembly, of association, of procession and of demonstration," CHINA. CONST. art. 35, *available at* http://english.peopledaily.com.cn/constitution/constitution.html (last visited Oct. 19, 2008).

29. ICCPR, *supra* note 28.

30. *Id.* art. 19(1).

31. *Id.* art. 19(2).

32. *Id.* art. 17(1).

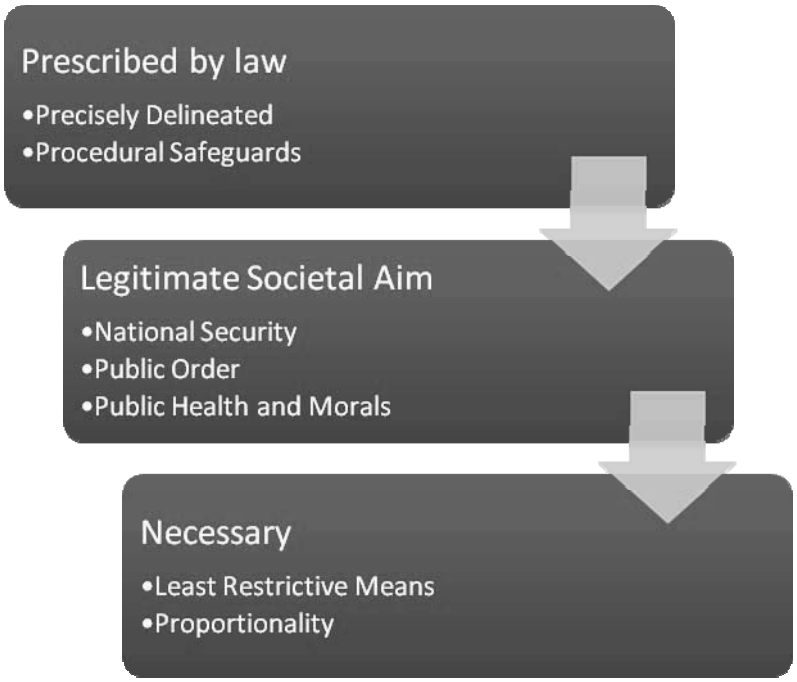
33. Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment, art. 2(2), Dec. 12, 1984, 23 I.L.M. 1027, as modified, 24 I.L.M. 535 (1985), June 26, 1987 - Oct. 21, 1994, 34 I.L.M. 590, 591 (1995), *available at* http://www.unhchr.ch/html/menu3/b/h_cat39.htm (last visited Nov. 11, 2008) ("No exceptional circumstances whatsoever . . . may be invoked as a justification of torture.").

34. ICCPR, *supra* note 28, at art. 19(3)(b).

35. United Nations Economic and Social Council, United Nations Sub-Comm. on the Prevention of Discrimination and Prot. of Minorities, *Siracusa Principles on the Limitation and Derogation of Provisions in the International Covenant on Civil and Political Rights*, UN Doc. E/CN.4/1984/4 (Sep. 28, 1984).

of the United Nations Human Rights Committee.[36] Still greater precision is provided by the decisions of international, regional, and national tribunals applying to concrete situations rights mirroring the guarantees of expression and privacy in the ICCPR.

From the above-identified sources of international human rights law, the following standard emerges: international human rights law prohibits ICTs from assisting governments in interfering with the rights to freedom of expression and privacy, except when *necessary* to further a *legitimate societal aim*, and the interference is *prescribed by law*.[37] The international legal requirements for interfering with freedom of expression and privacy are depicted graphically and explained in detail below.



a) Interferences Must Be Prescribed By Law

A threshold requirement for the lawfulness of any restriction on the freedom of expression or privacy is that it be "prescribed by law."[38] Satisfaction of this condition requires not only that national law provide for the

36. Human Rights Committee, General Comment 16, (Twenty-third session, 1988), Compilation of General Comments and General Recommendations Adopted by Human Rights Treaty Bodies, U.N. Doc. HRI/GEN/1/Rev.6 at 142 (2003).

37. "Exploring the Contours of the Rights to Freedom of Expression and Privacy on the Internet," Memorandum, *Berkeley Law International Human Rights Clinic* 26 (March 15, 2007) [hereinafter *Berkeley Memorandum*] (on file with author).

38. *Siracusa Principles, supra* note 35, ¶ 15.

restriction at the relevant time, but that such law is not "arbitrary or unreasonable."[39] To guard against arbitrariness, tribunals have required that laws restricting privacy be precise and narrowly tailored.[40] The United Nations Human Rights Committee has further elaborated:

> legislation must specify in detail the precise circumstances in which such interferences may be permitted. A decision to make use of such authorized interference must be made only by the authority designated under the law, and on a case by case basis.[41]

National laws enabling interferences with privacy and expression must also contain sufficient procedural safeguards and remedies to guard against abuse.[42] In cases where private communications are monitored, courts evaluating the sufficiency of procedural safeguards have often required approval by a judicial body, such as the issuance of a warrant.[43]

The "prescribed by law" requirement provides ICTs a relatively objective means of evaluating government directives to take actions that interfere with privacy and expression. If national law does not provide for the specific interference, it is *prima facie* arbitrary. Likewise, laws lacking the requisite specificity and safeguards—requiring filtering of broad categories of content or surveillance of Internet communications on a generalized basis without adequate procedural safeguards, for example—are inconsistent with international human rights law.

b) Interferences Must Further A Legitimate Societal Aim

International human rights law permits interferences with privacy and expression only to the extent they further a legitimate aim of the state.[44] Legitimate aims include: "national security," "public order" and "public health or morals."[45] These otherwise broad categories have been precisely defined by international bodies[46] and narrowly construed by courts.[47]

---

39. *Id.* ¶ 16.

40. Malone v. The United Kingdom, 8691/79 Eur. Ct. H.R. 10, ¶ 68 (1984); Kruslin v. France, 11801/85 Eur. Ct. H.R. 10, ¶ 33 (1990); *Berkeley Memorandum*, *supra* note 37, at 35.

41. *See* United Nations Human Rights Committee, General Comment No. 16, *supra* note 36, ¶ 8.

42. *Siracusa Principles*, *supra* note 35, ¶¶ 31, 34, 70.

43. *Berkeley Memorandum*, *supra* note 37, at 41.

44. *Siracusa Principles*, *supra* note 35; *Berkeley Memorandum*, *supra* note 37.

45. ICCPR, *supra* note 28, art. 19(3).

46. *Siracusa Principles*, *supra* note 35, ¶¶ 29-32 (national security), 22-24 (public order, 25-26 (public health), 27-28 (public morals).

47. *See e.g.*, Sunday Times v. UK (No. 1), Eur. Ct. H.R., Series A No. 30 (1979) (observing that exceptions to the freedom of expression guaranteed by European Conven-

National security is an extremely narrow ground for interference, applicable only in the face of existential threats to the state. The *Sircausa Principles* define its limited scope: "National security may be invoked to justify measures limiting certain rights only when they are taken to protect the existence of the nation or its territorial integrity or political independence against force or threat of force."[48] "[M]erely local or relatively isolated threats to law and order" do not, therefore, justify interference.[49] Moreover, national security may only be invoked to restrict privacy and expression when accompanied by sufficient procedural safeguards and remedies to guard against abuse.[50]

Importantly, political speech critical of the government, the system of government, or even advocating for non-violent political change, may not be restricted on national security grounds.[51] Human rights tribunals have held that governments must endure a high level of public scrutiny and criticism.[52]

Public order is defined as "the sum of rules which ensure the functioning of society or the set of fundamental principles on which society is founded."[53] The *Siracusa Principles* further specify that, because respect for human rights forms a part of public order, public order must be "interpreted in the context of the purpose of the particular human right which is limited on this ground."[54]

Public health may be invoked to limit certain rights when necessary to address "serious threat[s] to the health of the population or individual[s]."[55] With respect to public morals, the *Siracusa Principles* clarify:

> Since public morality varies over time and from one culture to another, a state which invokes public morality as a ground for restricting human rights, while enjoying a certain margin of discretion, shall demonstrate that the limitation in question is *essential*

---

tion on Human Rights shall be narrowly construed); *Berkeley Memorandum, supra* note 37, at 26.

48. *Siracusa Principles, supra* note 35, ¶ 29.

49. *Id.* ¶ 30.

50. *Id.* ¶ 31.

51. Johannesburg Principles on National Security, Freedom of Expression and Access to Information, principle 7(a), 1996, U.N. Doc. E/CN.4/1996/39.

52. Castels v. Spain, 1798/85 Eur. Ct. H.R. 48 (1992); Exploring the Contours of the Rights to Freedom of Expression and Privacy on the Internet," *Berkeley Memorandum, supra* note 37, at 27.

53. *Siracusa Principles, supra* note 35, ¶ 22.

54. *Id.* ¶ 23.

55. *Id.* ¶ 25.

> to the maintenance of respect for fundamental values of the community.[56]

c) Interferences Must Be Necessary

Interferences with privacy and expression rights must not only further a legitimate societal aim, but be *necessary* to its achievement.[57] To fulfill the necessity requirement, interferences must be as narrow as possible and proportionate to the societal interest at stake.[58] The necessity requirement substantially parallels the U.S. Supreme Court's "least restrictive means" jurisprudence with respect to the First Amendment.[59] It is doubtful that blanket-filtering requirements to restrict access to broad categories of information will *ever* satisfy the necessity requirement. It is likewise doubtful that, even where legitimately restricted content is identified precisely, blunt technological means for filtering (URL-level filtering, for example) will satisfy this narrow necessity requirement.

In addition to narrowness, the European Court of Human Rights has interpreted the *proportionality* component of necessity to require a high degree of causal certainty that failure to restrict the expression targeted by the government would in fact have the adverse societal consequences asserted.[60] Because Internet filtering constitutes a prior restraint on expression,[61] "call[ing] for the most careful scrutiny,"[62] it follows that filtering

---

56. *Id.* ¶ 27 (emphasis added).

57. *See* European Convention for the Protection of Human Rights and Fundamental Freedoms, arts. 8(2) (privacy) and 10(2), Nov. 4, 1950, 4.XI.1950 U.N.T.S. 222 (permitting interference with these rights only as "necessary in a democratic society . . ."); ICCPR, supra note 28, at art. 19(3); *Siracusa Principles*, *supra* note 35, ¶ 10.

58. *Siracusa Principles*, *supra* note 35, ¶ 10.

59. *Berkeley Memorandum*, *supra* note 37, at 31. *See also* Reno v. ACLU, 521 U.S. 844, 874 (1997) (applying the least restrictive means test and striking down two provisions of the Communications Decency Act of 1996 aimed at shielding children from obscene material on the Internet).

60. *See* Sunday Times v. UK (No. 1), Eur. Ct. H.R., Series A No. 30, ¶¶ 65-67 (1979) (considering the consequences of dissemination of information subject to an injunction, and comparing these consequences to the public interest in access to the information).

61. *See* Ctr. for Democracy & Tech. v. Pappert, 337 F.Supp.2d 606, 656 (E.D. Pa. 2004) (holding that a statutory procedure requiring ISPs to remove offensive content *without prior judicial determination* was an administrative prior restraint). As traditionally defined, prior restraint refers to orders forbidding certain communications that are issued before the communications occur. Alexander v. United States, 509 U.S. 544, 549 (1993). Yet the Supreme Court has also deemed state-mandated *removal* of protected expression from circulation to be an "administrative prior restraint." Bantam Books Inc., v. Sullivan, 372 U.S. 58, 70-71 (1963).

62. Observer v. United Kingdom, 13585/88 Eur. Ct. H.R. 49, ¶ 60 (1991)

will only be permissible where the blocked information is almost certain to cause harm to a legitimate societal interest.

2. Standards of Accessorial Liability for State Persecution

Yahoo!'s provision of Shi Tao's identifying information to Chinese authorities was inconsistent with his internationally protected right to privacy because the vagueness of the "state secrets" assertion was not sufficient to justify this interference on national security grounds.[63] Yet when Chinese authorities, enabled by this information, kidnapped, arbitrarily detained, and tortured Shi Tao, Yahoo! became exposed to accessorial liability for these human rights abuses. Unlike the violation of Shi Tao's right to privacy, these human rights violations are actionable in U.S. federal courts.

The Alien Tort Claims Act (ATCA) grants federal district courts subject matter jurisdiction over "civil action[s] by an alien for a tort only, committed in violation of the law of nations or a treaty of the United States."[64] Originally enacted as part of the Judiciary Act of 1789, this provision lay dormant for nearly two centuries until successfully invoked by citizens of Paraguay to hold Paraguayan officials civilly liable for grave human rights violations.[65] The statute has since been employed by victims of human rights abuses to sue both state officials[66] and transnational corporations[67] in U.S. federal courts.

The Supreme Court has addressed the ATCA only once, in *Sosa v. Alavarez-Machain*.[68] In a decision that perhaps raised as many uncertainties as it resolved, the Supreme Court at once confirmed the viability of the ATCA and defined the limits of its reach. The ACTA was solely a jurisdictional grant, the Supreme Court clarified, and does not supply a cause of action.[69] A cause of action must come from the "law of nations:" customary international law or treaties to which the United States is a par-

63. *See supra*, Section I.B.1.c).

64. 28 U.S.C. § 1350.

65. Filartiga v. Pena-Irala, 630 F.2d 876 (2d Cir. 1980). On remand, the district court for the Eastern District of New York awarded compensatory and punitive damages as well as attorney fees to Plaintiffs for the torture and death of their brother and son. Filartiga v. Pena-Irala, 577 F.Supp. 860 (E.D.N.Y. 1984).

66. *See, e.g.*, *In re* Estate of Marcos, 25 F.3d 1467 (9th Cir. 1994) (ATCA suit against the former President of the Philippines).

67. *See, e.g.*, Khulumani v. Barclay Nat'l Bank Ltd., 504 F.3d 254 (2d Cir. 2007) *aff'd* without opinion, 128 S. Ct. 2424 (2008) (ATCA suit against banks for aiding and abetting Apartheid in South Africa).

68. 542 U.S. 692 (2004).

69. *Id.* at 714.

ty. *Sosa* further clarified that only a "narrow class" of international norms "accepted by the civilized world and with a specificity comparable to the features of the 18th-century paradigms recognized by the court" are actionable under the ATCA.[70] This "narrow class" of international norms[71] includes, *inter alia*, torture, extrajudicial killing,[72] and prolonged arbitrary detention in some circumstances.[73]

That ICT companies would commit these grave human rights abuses is of course almost beyond contemplation.[74] Moreover, because these offenses only violate the "law of nations" when committed by or with a

---

70. *Id.* at 725, 729.

71. *See* RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW OF THE UNITED STATES § 702 (1987) ("A state violates international law if, as matter of state policy, it practices, encourages or condones . . . (c) murder . . . (d) torture . . . (e) prolonged arbitrary detention . . . .").

72. Definitions of torture and extrajudicial killing are found in the Torture Victim Protection Act of 1991 (TVPA), 28 U.S.C. § 1350 (note). Extrajudicial killing is defined as:

[A] deliberated killing not authorized by a previous judgment pronounced by a regularly constituted court affording all the judicial guarantees which are recognized as indispensable by civilized peoples. Such term, however, does not include any such killing that, under international law, is lawfully carried out under the authority of a foreign nation.

Torture is defined in part as:

[A]ny act, directed against an individual in the offender's custody or physical control, by which severe pain or suffering (other than pain or suffering arising only from or inherent in, or incidental to, lawful sanctions), whether physical or mental, is intentionally inflicted on that individual for such purposes as obtaining from that individual or a third person information or a confession, punishing that individual for an act that individual or a third person has committed or is suspected of having committed, intimidating or coercing that individual or a third person, or for any reason based on discrimination of any kind.

This definition of torture is virtually identical to that in Article 1 of the Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment, *supra* note 33.

73. Arbitrary detention is "detention of an individual not pursuant to law." Ralph G. Steinhardt, *Laying One Bankrupt Critique to Rest:* Sosa v. Alvarez-Machain *and the Future of International Human Rights Litigation in U.S. Courts*, 57 VAND. L. REV. 2241, 2300 (2004). It must be acknowledged that the Supreme Court held in *Sosa v. Alvarez-Machain* that "a single illegal detention of less than a day, followed by the transfer of custody to lawful authorities and a prompt arraignment" was not actionable under the ATCA. 542 U.S. at 738. However, § 702 THE RESTATEMENT (THIRD) ON FOREIGN RELATIONS LAW OF THE UNITED STATES specifies that *prolonged* arbitrary detention violates international law, and it is therefore likely that arbitrary detention for longer periods will be actionable under the ATCA.

74. The possibility seems especially remote given that ICT employees technically need not even be present in all countries in which they operate; Internet and communication products and services can be made available literally with the flip of a switch.

state,[75] they would not be actionable in U.S. courts under ATCA if carried out entirely by ICTs without state involvement. Rather, ICTs face accessorial liability under the ATCA for aiding and abetting human rights violations committed by states. ICTs expose themselves to such liability when they provide state authorities with user-identifying information, with knowledge that the state intends to use the information to commit human rights violations. The ATCA aiding and abetting standards articulated below are of great importance to ICTs because, unlike the ultimate offenses carried out by states, aiding and abetting concerns conduct within the control of companies.

a) Aiding and Abetting Standard

A broad consensus exists among courts[76] and commentators[77] that corporations may be liable for aiding and abetting grave international law violations committed by states. Beyond this, the consensus fractures into divergent approaches to the *source* and *content* of the standard for aiding and abetting liability under the ATCA. This split exists not only between circuits, but within appellate panels. In *John Doe I v. Unocal Corporation*, the Ninth Circuit agreed that private corporations may be accessorily liable under the ATCA for human rights abuses committed by states.[78] Judge Pregerson's majority held that the standard for aiding and abetting in ATCA cases is found in international law.[79] Looking principally to the constitutive statutes of the International Criminal Tribunals for the Former Yugoslavia and Rwanda and the jurisprudence of these tribunals—as evidence of customary international law—the *Unocal* majority held that aiding and abetting liability can be imposed for "knowing practical assistance or encouragement which has a substantial effect on the perpetration of the crime."[80]

---

75. Certain international norms, such as the prohibition on genocide or piracy, however, do not require state action to constitute a violation of international law. *See, e.g.*, Kadic v. Karadzic, 70 F.3d 232, 239 (2d Cir. 1995).

76. Khulumani v. Barclay Nat'l Bank Ltd., 504 F.3d 254, 260 (2d Cir. 2007), *aff'd* without opinion, 128 S. Ct. 2424 (2008); John Doe I v. Unocal Corp., 395 F.3d 932, 951 (9th Cir. 2002) *vacated by* 395 F.3d 978 (9th Cir. 2003); Bowoto v. Chevron Corp., No. C99-02506, 2006 U.S. Dist. LEXIS 63209, 18-19 (N.D. Cal. Aug. 26, 2006).

77. *See, e.g.*, Brief of International Law Scholars as Amici Curiae, Khulumani v. Barclay Nat'l Bank Ltd., 504 F.3d 254 (2d Cir. 2007); Chimène I. Keitner, CONCEPTUALIZING COMPLICITY IN ALIEN TORT CASES, 60 HASTINGS L.J. __ (forthcoming 2008).

78. 395 F.3d at 962-63.

79. *Id.* at 947.

80. *Unocal*, 395 F.3d at 947. Judge Pregerson derived this standard principally from the ICTY's decision in Prosecutor v. Furundzija, IT-95-17/1-T (Dec. 10, 1998), *reprinted in* 38 I.L.M. 317 (1999).

Judge Reinhardt concurred in the existence of accessorial liability, but maintained that federal judges, in ascertaining the correct standard, should "look to traditional civil tort principles embodied in federal common law, rather than to evolving standards of international law."[81] A similar divide emerged from the Second Circuit in *Khulumani v. Barclay Nat'l Bank Ltd.*,[82] the most recent appellate decision to grapple with accessorial liability of corporations under the ATCA. Despite their agreement that aiding and abetting survived the Supreme Court's *Sosa* decision and remains a viable theory of liability, Judges Katzmann and Hall could not agree as to the appropriate source of the standard. Judge Katzmann engaged in an extensive survey of customary international law before concluding that the appropriate standard is found in Article 25(3)(c) of the Rome Statute of the International Criminal Court.[83] Judge Katzmann articulated the following standard:

> [A] defendant may be held liable under international law for aiding and abetting the violation of that law by another when the defendant (1) provides practical assistance to the principal which has a *substantial effect* on the perpetration of the crime, and (2) does so with the *purpose* of facilitating the commission of that crime.[84]

Judge Hall disagreed as to both the source and content of this standard. In Judge Hall's view, "a federal court should resort to its traditional source, the federal common law, when deriving the standard."[85] Looking to the common law, Judge Hall identified Section 876(b) of the Restatement (Second) of Torts as the appropriate standard for aiding and abetting under the ATCA. According to this standard, a corporation aids and abets if it "knows that the other's conduct constitutes a breach of duty and gives substantial assistance or encouragement to the other."[86] Applying Section 876(b) of the Restatement to ATCA civil aiding and abetting claims, Judge Hall explained that "liability should be found only where there is evidence that a defendant furthered the violation of a clearly established

---

81. *Unocal*, 395 F.3d at 965 (Reinhardt, J., concurring). Judge Reinhardt identified three common law theories of accessorial liability: joint venture, agency, and reckless disregard. *Id.* at 969.

82. 504 F.3d 254, 256 (2d Cir. 2007).

83. *Id.* at 275-77 (Katzmann, J., concurring).

84. *Id.* at 277 (emphasis supplied).

85. *Id.* at 286 (Hall, J., concurring).

86. *Id.* at 287 (Hall, J., concurring) (quoting RESTATEMENT (SECOND) OF TORTS, § 876(b) (1979)).

international law norm in one of three ways," the first being most directly relevant to ICT operations:

> (1) by knowingly and substantially assisting a principal tortfeasor, such as a foreign government or its proxy, to commit an act that violates a clearly established international law norm; (2) by encouraging, advising, contracting with, or otherwise soliciting a principal tortfeasor to commit an act while having actual or constructive knowledge that the principal tortfeasor will violate a clearly established customary international law norm in the process of completing that act; or (3) by facilitating the commission of human rights violations by providing the principal tortfeasor with the tools, instrumentalities, or services to commit those violations with actual or constructive knowledge that those tools, instrumentalities, or services will be (or only could be) used in connection with that purpose.[87]

The disagreement as to the appropriate source of the aiding and abetting standard is doubtless due to the existence of suitable standards *both* at common law and in customary international law,[88] and persuasive arguments supporting the primacy of either.[89] Yet for ICTs seeking to order their affairs to avoid ATCA liability, the source of the standard is of little importance; it is the *content* that determines whether or not their conduct falls within the scope of aiding and abetting. In this sense, the aiding and abetting standards applied in ATCA cases from both international and federal common law are very similar.[90] The material difference is whether it is sufficient that a company, at the time it provides assistance, has *knowledge* of the government's intent to engage in torture, extrajudicial killing or arbitrary detention, or whether the company must act with the *purpose* of facilitating these grave human rights violations. To illustrate the outcome-determinative difference of the knowledge and purposefulness stan-

---

87. *Id.* at 288-89 (Hall, J., concurring).

88. Brief of International Law Scholars as Amici Curiae, *Khulumani v. Barclay Nat'l Bank Ltd*., 504 F.3d 254 (2d Cir. 2007) *available at* http://www.cmht.com/pdfs/SAACLawScholars083005.pdf.

89. *See id.* (Demonstrating the existence of suitable standards for aiding and abetting both in customary international law and the federal common law, and articulating the case for the latter); Chimène I. Keitner, *Conceptualizing Complicity In Alien Tort Cases*, 60 HASTINGS L.J. __ (forthcoming 2008) (arguing that doctrinal coherence dictates that customary international law is the appropriate source of the standard for aiding and abetting).

90. Indeed, in identifying the standard for the majority in *Doe v. Unocal*, Judge Pregerson consciously adjusted the customary international law formulation so as to bring it in line with the common law standard codified in Section 876(b) of the Restatement (Second) of Torts. *See* 395 F.3d at 951.

dards in a likely scenario, each is applied to the Shi Tao case below.[91] Because Yahoo! settled the case before any judgment on the merits of the ATCA claims, it is instructive to work through the merits of the claims here.

b) Application of Aiding and Abetting Standards to the Shi Tao Case

The factual circumstances of the Shi Tao case represent the most likely scenario in which a U.S. ICT company would be exposed to ATCA liability. Applying the knowledge standard—and assuming plaintiffs were able to prove the factual allegations of arbitrary detention and torture—it is possible that Yahoo! would have been held liable under the ATCA for aiding and abetting these acts of the Chinese government. That the internationally proscribed acts were committed by the Chinese government satisfies international law's state action requirement.[92] Moreover, a reasonable fact finder could probably find that the company's provision of personally identifiable information—without which Shi Tao presumably could not have been identified—fulfills the "substantial effect" element of the aiding and abetting standards.[93] Aiding and abetting liability would thus turn on whether plaintiffs could prove that Yahoo! *knew* that the Chinese government intended to kidnap and torture Shi Tao at the time it handed over the

91. Plaintiffs in the Shi Tao case asserted several claims in addition to those under the ACTA, including claims under the Torture Victim Protection Act of 1991 (TVPA), 28. U.S.C. § 1350 (note), The Electronic Communications Privacy Act, 18 U.S.C. § 2701 *et seq.* (2006), and California Business & Professional Code §§ 17200 *et seq.* It is noteworthy that there is a split of authority as to whether the term "individual" in the TVPA encompasses corporations, or is limited to natural persons. Two California district courts recently held that the TVPA does not apply to corporations. Mujica v. Occidental Petroleum Corp., 381 F. Supp. 2d 1164, 1175-76 (C.D. Cal. 2005) (observing that the TVPA's use of the word "individual" to describe *both* the perpetrator and object of torture, and reasoning that a corporation cannot be the object of torture); Bowoto v. Chevron Corp., 2006 U.S. Dist. LEXIS 63209, 6 (N.D. Cal. 2006). *But see*, Sinaltrainal v. Coca-Cola Co., 256 F. Supp. 2d. 1345, 1358-59 (S.D. Fla 2003) (holding that "individual" as used in the TVPA includes corporations); Estate of Rodriquez v. Drummond Co., Inc., 256 F. Supp. 2d. 1250, 1267 (N.D. Ala. 2003) (same).

92. Note that in the case of international norms requiring state action, a private actor may be liable as an aider and abettor of an offense for which it could not be the principal. For purposes of ATCA liability, this technicality is "of no moment." *Khulumani*, 504 F.3d at 281-82, 289.

93. A decision of the Nuremberg Tribunal—evidencing international custom—established that provision of identifying information, coupled with the knowledge that the identified individuals would be executed upon discovery, was sufficient to convict the defendant as an accessory. United States v. Ohlendof, 4 TRIALS OF WAR CRIMINALS BEFORE THE NUREMBERG MILITARY TRIBUNALS UNDER CONTROL COUNCIL LAW No. 10, 1, 569 (1949), cited in Brief of Int'l Law Scholars, *supra* note 88.

user information. Plaintiffs attempted to imply such knowledge from public reports that Chinese dissidents routinely faced arbitrary detention and torture, and particularly from a 2002 letter from Human Rights Watch, addressed to Yahoo! executives, warning the company of these conditions and that "[t]here is a strong likelihood that Yahoo will assist in furthering such human rights violations."[94] Whether Yahoo! had sufficient knowledge at the relevant time would have likely been at least a disputed question of material fact, and allowed the Plaintiffs to present their case to a jury. In any case, in the aftermath of the Shi Tao case, it will be difficult for ICTs to deny a *general* knowledge of the possible consequences of their actions. This general knowledge, while probably not sufficient for liability, may elevate ICTs' duty of care in responding to government demands for user information.

By contrast, it is highly unlikely that Yahoo! would have been found liable under the purposefulness standard for aiding and abetting. Whereas an argument can at least be made that Yahoo! knew the Chinese government intended to persecute the subject of its "state secrets" inquiry, there is no indication that Yahoo! furnished the user information *with the purpose of facilitating* acts of torture and arbitrary detention. Nor is it foreseeable that ICTs would act with such purpose. Allegations of purposeful aiding and abetting of human rights violations have thus far involved companies conspiring with governments to protect their physical investments[95]—a factual scenario not particularly relevant to ICTs.

Yet ICTs, in assessing risk and formulating policies for responding to government requests for user information, should plan as though their conduct will be judged against a knowledge standard for aiding and abetting. Although federal courts are not at this time bound to apply the knowledge standard as a matter of precedent, the weight of persuasive authority points in this direction. In *Doe I v. Unocal Corp.*, all three judges on the Ninth Circuit panel applied a knowledge standard, albeit from difference sources.[96] The decision lacks precedential force—it was vacated by an or-

---

94. *Shi Tao complaint*, *supra* note 6 at ¶ 29; Letter from Kenneth Roth, Executive Director, Human Rights Watch, to Terry Semel, Chairman and CEO, Yahoo! Inc. (Jul. 30, 2002) *available at* http://www.hrw.org/press/2002/08/yahoo-ltr073002.htm.

95. *See Unocal*, 395 F.3d. 932 (9th Cir. 2002) (Burmese villagers alleged murder, rape, torture and forced labor in connection with the construction of a gas pipeline); *Bowoto*, 2006 U.S. Dist. LEXIS 63209 (N.D. Cal. 2006) (Involving human rights violations committed by Nigerian security forces against protesters on a Chevron oil platform).

96. 395 F.3d 932. Writing for the majority, Judge Pregerson, joined by Judge Tashima, applied a knowledge standard sourced from international law. *Id.* 947. Concurring Judge Reinhardt identified three federal common law theories of accessorial liability: joint venture, agency, and reckless disregard. *Id*. at 969. Reckless disregard is most rele-

der granting an *en banc* rehearing, and the case settled before rehearing[97]—but the District Court for the Northern District of California recently applied this standard in *Bowoto v. Chevron*.[98] Judge Katzmann's concurrence in the Second Circuit's *Khulumani* decision remains the only support for a purposefulness standard, and there is reason to doubt its adoption by other courts. Acknowledging that international criminal tribunals apply a knowledge standard, Judge Katzmann nevertheless concluded that such a standard is insufficiently "well-established and universally recognized," "particularly in light of the higher standard articulated in the Rome Statute."[99] Yet it is not clear that the Rome Statute does articulate a higher standard: subsection (d)(ii) of the Article cited by Judge Katzmann states a knowledge standard.[100] Judge Katzmann's position does not seem to be that the knowledge standard adopted by international criminal tribunals is not well-established so much as the narrower standard he adopts is *more* well-established.[101] There remains a substantial likelihood that judges looking to international law for an ATCA aiding and abetting standard will be satisfied with the knowledge standard's prevalence in international criminal jurisprudence, as were the Ninth Circuit in *Doe v. Unocal* and the Northern District of California in *Bowoto v. Chevron*. Where judges look instead to the federal common law, the knowledge standard of

---

vant to ICT operations and, like the knowledge standard articulated by the majority, does not require purposefulness. *Id.* at 975. Reckless disregard "occurs when a party is aware of (or should be aware of) an unreasonable risk, yet disregards it, thereby leading to harm to another." *Id*. at 974.

97. Doe I v. Unocal Corp., 395 F.3d 978 (9th Cir. 2003) (granting rehearing en banc), *vacated*, 403 F.3d 708 (9th Cir. 2005) (granting parties' stipulated motion to dismiss).

98. 2006 U.S. Dist. LEXIS 63209, 18-19 (N.D. Cal. 2006).

99. *Khulumani*, 504 F.3d at 278-79 (Katzmann, J., concurring).

100. Article 25 of the Rome Statute of the International Criminal Court provides in relevant part:

(c) For the purpose of facilitating the commission of such a crime, aids, abets or otherwise assists in its commission or its attempted commission, including providing the means for its commission;

(d) In any other way contributes to the commission or attempted commission of such a crime by a group of persons acting with a common purpose. Such contribution shall be intentional and shall either:

(i) Be made with the aim of furthering the criminal activity or criminal purpose of the group, where such activity or purpose involves the commission of a crime within the jurisdiction of the Court; or

(ii) Be made in the knowledge of the intention of the group to commit the crime;

Rome Statute of the International Criminal Court, July 17, 1988, 2187 U.N.T.S. 90, *available at* http://untreaty.un.org/cod/icc/statute/romefra.htm.

101. *Khulumani*, 504 F.3d at 277 n. 12 (Katzmann, J., concurring).

Section 876(b) of the Restatement will most likely apply. In either case, ICTs expose themselves to risk of aiding and abetting liability when they provide identifying user information to a state actor with knowledge that it intends to arbitrarily detain, torture, or summarily execute the identified user.

C. Consequences of Noncompliance

The spectrum of consequences for noncompliance with the global law divides into two categories: legal and non-legal consequences. The availability of civil damages is familiar, although it may come as a surprise to some that ICTs may be civilly liable in U.S. courts for human rights violations committed by foreign governments. Such legal consequences will only arise in cases in which ICTs knowingly enable grave human rights abuses. A separate set of non-legal consequences flow from ICT interference with free expression and privacy rights. Although less immediate than civil damages, these consequences may substantially impair their long-term competiveness.

Although not actionable in U.S. courts,[102] ICT interference with free expression and privacy rights—such as filtering Internet content or intercepting communications—carries consequences that may be equally harmful to ICTs' long-term interests. ICT operations are subject to constant, global scrutiny enabled in part, somewhat ironically, by their own technologies. NGOs such as Human Rights Watch, Amnesty International, and Reporters Without Borders have carefully monitored the human rights implications of ICT operations in repressive states, and generated public awareness through reports[103] and press releases[104] detailing ICT interferences with fundamental human rights. Mainstream media outlets such as the New York Times[105] and the BBC[106] have broadcast NGO allegations

102. In *Sosa*, the Supreme Court held that the ICCPR could not supply a cause of action under the ATCA because the treaty is not self-executing. Sosa v. Alvarez-Machain, 542 U.S. 692, 735 (2004). It is not likely that a U.S. court would recognize customary international law rights of privacy and expression as being sufficiently definite to be actionable under the ATCA.

103. *See, e.g.*, Human Rights Watch, *supra* note 3; AMNESTY INT'L, UNDERMINING FREEDOM OF EXPRESSION IN CHINA: THE ROLE OF YAHOO!, MICROSOFT AND GOOGLE, (2006); Reporters Without Borders, *supra* note 15.

104. *See, e.g.*, Press Release, Human Rights Watch, China: Internet Companies Aid Censorship, Aug. 8, 2006, *available at* http://www.hrw.org/en/news/2006/08/08/china-internet-companies-aid-censorship.

105. *See, e.g.*, Kristof, Yahoos, *supra* note 16; Tina Rosenberg, *Building the Great Firewall of China, With Foreign Help*, N.Y. TIMES, Sep. 18, 2005, § 4 at 11.

106. *See, e.g.*, Nembi Mutch, *Net Giants 'Still Failing China,'* BBC NEWS, Dec. 18, 2006, http://news.bbc.co.uk/2/hi/technology/6191171.stm (last visited Dec. 20, 2008).

worldwide, and bloggers have cited human rights abuses as evidence that the once-infallible technology giants are in fact no different than "evil" corporate America.[107] Yahoo! has suffered the most intense public scrutiny in part because of the grave human rights abuses endured by Shi Tao and Wang Xiaoning, and because they were defendants in an ATCA suit for these abuses in the Northern District of California.

ICT operations in China have also been the subject of scrutiny by both houses of Congress. Members of the House Committee on International Relations questioned executives of Yahoo!, Google, Microsoft and Cisco about their China operations in February 2006.[108] After an NGO published online the Bejing State Security Bureau's request for Shi Tao's identifying information[109]—which contradicted Yahoo! General Counsel Michael Callahan's prior testimony that the company was not aware of the nature of the request[110]—Yahoo! executives were again summoned to testify in a hearing titled: "Yahoo! Inc.'s Provision of False Information To Congress."[111] Most recently, in May 2008, Yahoo!, Google, Microsoft and Cisco testified before the Senate Subcommittee on Human Rights and the Law, which urged the companies to quickly move forward with a code of conduct.[112]

Because the international rights to freedom of expression and privacy mirror sacred guarantees in the United States Constitution, allegations of their abuse carry particular moral force. This may be even more true in the progressive, globally-minded communities in northern California and Washington that are home to leading ICTs and many of their stakeholders. That international human rights are expressed as *law*—codified in treaties, and enforced by international tribunals—means that even extrajudicial allegations of human rights abuses are made, and judged, within a quasi-legal framework wherein the NGOs play the prosecutorial role, and frame their allegations according to international norms. The "jury" includes ICT stakeholders such as users, investors, business partners, employees and

---

107. *See, e.g.*, Iain Thompson, *Google hands over user information in India: 'do no evil' motto looking increasingly strained*, vunet.com, May 20, 2008, http://www.vnunet.com/vnunet/news/2217063/google-handing-user-information (last visited Feb 2, 2009).

108. Internet in China, *supra* note 18.

109. Beijing State Security Bureau, *supra* note 1.

110. Internet in China, *supra* note 18 (Testimony of Michael Callahan, General Counsel of Yahoo! Inc.).

111. Yahoo! Inc.'s Provision of False Information to Congress, Hearing Before H. Comm. On Foreign Affairs, 110th Cong. (2007).

112. Global Internet Freedom: Corporate Responsibility and the Rule of Law, Hearing Before S. Subcomm. on Human Rights and the Law, 110th Cong. (2008) (Opening Statement of Chairman Senator Dick Durbin).

their families. These parties ultimately reach a verdict of "right" or "wrong."[113] This is not to say that the public dialog following allegations of human rights abuses is conducted with the evidentiary discipline of the courtroom. Rather, it shows that many international human rights are familiar and somewhat intuitive in western, liberal democracies. It is against this intuitively-understood standard that ICTs are judged.

Public association with human rights abuses impairs two of ICT companies' most valuable assets: their brand and human capital. These assets are uniquely valuable to ICT companies, making them more sensitive to the non-legal consequences of human rights violations than other sectors of the economy.

1. Brand Consequences

The brands of the leading ICTs are among the most valuable in the world: Interbrand's 2008 rankings value the Microsoft brand at $59 billion in third place, Google's at $25.5 billion in tenth place, and Yahoo's at $5.5 billion in sixty-fifth place.[114] Trust, a component of brand value, is vitally important to ICT companies.[115] Google's Code of Conduct goes so far as to state: "Our reputation as a company that our users can trust is our most valuable asset, and it is up to all of us to make sure that we continually earn that trust."[116] Professor Tim Wu agrees with Google's assessment, observing: "One reason [Google is] good at the moment is they live and die on trust, and as soon as you lose trust in Google, its over for them."[117] Users necessarily entrust their private communications and user data to ICTs. It is not difficult to imagine that the way a company handles demands by one government to restrict content or turn over user information will affect the trust of users worldwide.

---

113. The accountability framework is somewhat different for ICT participants in The Global Network Initiative, the subject of Part II below. International human rights standards are incorporated into a code of conduct. Adherence to these standards is publicly judged through a process of independent assessments.

114. Interbrand, "Best Global Brands List 2008," http://www.interbrand.com/best_global_brands.aspx?langid=1000.

115. Geoff Lye, Google: Don't Be Evil, SustainAbility *Radar*, December 2005/January 2006 Issue, http://www.sustainability.com/downloads_public/insight_radar/leader_article1.pdf.

116. Google, *Code of Conduct*, http://investor.google.com/conduct.html (last visited Mar. 1, 2009).

117. Jeffrey Rosen, *Google's Gatekeepers*, N.Y. TIMES, Nov. 30, 2008, at MM50.

2. Human Capital Consequences

A company's brand—the images evoked by its trademark—is also important for recruiting.[118] The long-term success of ICT companies, perhaps more than any other business, depends on their ability to recruit, motivate and retain the very best of a highly educated workforce. ICTs compete on their ability to innovate: to continually push the limits of technology, design and business models. To attract and retain the creative minds to fuel this engine of innovation, ICTs offer employment perks unmatched by any industry.[119] Google's legendary perks in particular have made it a career destination.[120] Yet as Google grows and the economy slows, Google's employee benefits have begun to look increasingly mortal.[121] As the rate at which it mints new millionaires declines, Google's "do no evil" ethos may become increasingly important in competing for talent.

Public association with human rights abuses almost certainly impairs ICTs' ability to recruit and motivate top talent. Two studies of students in top MBA programs demonstrate that social responsibility factors prominently in employer preferences.[122] For the MBA students surveyed, the ethical reputation of a company was the fourth-most-important consideration, and approximately 70% reported willingness to forego financial benefit to work for an employer that respects outside stakeholders.[123] It is likewise conceivable that employee enthusiasm and pride that underpins productivity and innovation—in which ICTs invest heavily—erodes when companies act contrary to the values of employees and their commu-

---

118. INTERBRAND, BEST GLOBAL BRANDS 2008, http://www.interbrand.com/images/BGB_reports/BGB_2008_US_Format.pdf.

119. On recruiting, Google Co-founder Larry Page has said, "Google is organized around the ability to attract and leverage the talent of exceptional technologists and business people." Google, "Google Jobs," http://www.google.com/support/jobs/bin/static.py?page=gettingintogoogle.html (last visited Feb. 7, 2009).

120. Google topped Fortune's "100 Best Companies to Work For" list in both 2007 and 2008. FORTUNE, "100 Best Companies to Work For 2008," http://money.cnn.com/magazines/fortune/bestcompanies/2008/ (last visited Dec. 19, 2008).

121. See, e.g., Joe Nocera, On Day Care, Google Makes a Rare Fumble, N.Y. TIMES, Jul. 5, 2008, at A1.

122. David B. Montgomery & Catherine A. Ramus, Including Corporate Social Responsibility, Environmental Sustainability, and Ethics in Calibrating MBA Job Preferences, Stanford Research Paper No. 1981 (2007), *available* at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1077439; David B. Montgomery & Catherine A. Ramus, Corporate Social Responsibility Reputation Effects on MBA Job Choice, Stanford Research Paper No. 1805 (2003), *available at* http://www.google.com/support/jobs/bin/static.py?page=about.html&about=top10.

123. Montgomery & Ramus, Including, *supra* note 122, at 14; Montgomery & Ramus, Corporate, *supra* note 122, at 14.

nity.[124] Pride in association with a leading technology company can be quickly replaced by shame when that company is associated with human rights abuses in the headlines. And, as Yahoo! executives learned—from Representative Tom Lantos' much publicized "moral pygmies" charge[125]—the humiliation of association with human rights abuses is felt most acutely at the highest levels.

The above does not, of course, prove that the involvement of Yahoo!, Google, and Microsoft in restrictions on free expression and privacy has prevented these companies from recruiting talented employees or caused users to reject their products. Empirical evidence is nonexistent at this point. But it does illustrate why these companies are *uniquely* sensitive to public association with human rights abuses. Over time, even minor blemishes to a brand have the potential to *measurably* alter the perceptions of key consumers and top talent, substantially affecting the long-term competitiveness of a company.

II. RESPONSES OF PRIVATE, GOVERNMENTAL, AND NONGOVERNMENTAL ACTORS

The Shi Tao case was a watershed event, sparking public awareness of both the human consequences of Internet repression and the quandary facing U.S. ICTs operating in repressive states. At the urging of Congress,[126] leading ICTs began a two-year collaboration with NGOs, academics, and investors leading ultimately to the Global Network Initiative in October 2008. The State Department established the Global Internet Freedom Task Force (GIFT) to coordinate interagency efforts to "address challenges to the freedom of expression and the free flow of information on the Internet."[127] And Representative Christopher Smith (R-NJ) introduced H.R.

---

124. *See* Pitts, *supra* note 21 (Former Nokia general counsel reflecting on the competitive advantages resulting from the company's social responsibility initiatives, including "energizing, motivating and recruiting stellar employees, spurring innovating designs and technologies, nurturing trust and enthusiasm among all stakeholders, and building the global brand that represented Nokia's remarkable success.").

125. The late Representative Tom Lantos said of Yahoo! senior executives, "while technologically and financially you are giants, morally you are pygmies." Internet in China, *supra* note 18.

126. Internet in China, *supra* note 18, at 4 (Rep. Smith remarked, "I, and many of my colleagues on both sides of the aisle, would welcome leadership by the corporations to develop a code of conduct which would spell out how they could operate in China and other repressive countries like Vietnam while not harming citizens and respecting human rights.").

127. Press Release, U.S. Dep't of State, State Summary of Global Internet Freedom Task Force (Dec. 20, 2006) (on file with author).

275: Global Online Freedom Act of 2007,[128] a bill that would jointly establish executive-branch mechanisms for promoting "Internet freedom" globally and delineate minimum standards for U.S. ICT companies[129] operating in "Internet Restricting Countries"[130] backed by civil and criminal sanctions. Title II of the proposed legislation proscribes both censorship of Internet content and the provision of personally identifiable information to the authorities of Internet-restricting countries. Section 201 prohibits U.S. businesses from "locating" within an Internet-restricting country "any electronic communication that contains any personally identifiable information." Section 202 prohibits U.S. businesses that collect personally identifiable information from providing such information "to any foreign official of an Internet-restricting country," except for "legitimate foreign law enforcement purposes as determined by the Department of Justice."[131]

Although endorsed by human rights NGOs Amnesty International and Reporters Without Borders, the Global Online Freedom Act has met fierce resistance on a number of fronts.[132] Opposition has come not only from industry groups, but from the Center for Democracy and Technology, which is concerned that the mandates of the proposed law would be unworkable for ICTs, and thus do "more harm than good" to Internet freedom.[133] With the passing of a powerful ally, Tom Lantos, the bill's passage in its present form appears doubtful.[134] Despite the uncertain future of the Global Online Freedom Act, the possibility of legislation remains. In a statement welcoming the Global Network Initiative, Senator Richard Durbin added, "Congress should follow the lead of the private sector by

---

128. Global Online Freedom Act of 2007, H.R. 275, 110th Cong. (2007).

129. "United States Businesses" includes both companies with their principal place of business with the U.S. and their foreign subsidiaries to the extent that the U.S. parent controls or cooperates with the foreign subsidiary. *Id.* § 3(11)(c).

130. "Internet Restricting Countries" are those designated as such by the President of the United States on an annual basis. *Id.* § 3(6).

131. "Legitimate foreign law enforcement purposes" is defined as "for purposes of enforcement, investigation, or prosecution by a foreign official based on a publicly promulgated law of reasonable specificity that proximately relates to the protection or promotion of the health, safety, or morals of the citizens of that jurisdiction." *Id.* § 8(A).

132. Bennet Kelley, *Cyber legislation part of Capitol's spring fever*. 28 JOURNAL OF INTERNET LAW 11 2008; Letter from Brian A. Benczkowski, Principal Deputy Assistant Attorney General, United States Department of Justice, to Howard L. Berman, Acting Chairman, House Committee on Foreign Affairs, (May 19, 2008) (on file with author).

133. Memorandum, Ctr. for Democracy & Tech., Analysis of the Global Online Freedom Act of 2008 [H.R. 275]: Legislative Strategies to Advance Internet Free Expression and Privacy around the World at 2 (May 2, 2008), *available at* http://www.cdt.org/international/censorship/20080505gofa.pdf.

134. Kelley, *supra* note 132.

considering Internet freedom legislation that would complement the code of conduct."[135] Members of the European Union Parliament have also proposed draft legislation modeled closely on the Global Online Freedom Act.[136] Whether internet freedom legislation will be enacted will likely depend on the success of the Global Network Initiative.

A. Global Network Initiative

The most promising response to the ICT quandary is the Global Network Initiative launched in October of 2008. With the stated mission of "protecting and advancing freedom of expression and privacy in information and communication technology," the Initiative is the result of a two-year collaboration among leading ICTs (Google, Yahoo! and Microsoft), human rights organizations, academics and investors.[137] The structure of the Initiative and the obligations of its members are set out in its three constitutive documents. The Principles on Freedom of Expression and Privacy[138] outline high-level obligations of participating companies to protect and advance the freedom of expression and privacy. The Principles are explicitly grounded in international human rights law; obligations are justified by reference to the provisions of the International Covenant on Civil and Political Rights and the Universal Declaration of Human rights discussed above.[139] A second document, the Implementation Guidelines,[140] delineates more precise, concrete obligations of participating companies. Whereas the Principles announce such broach duties as to "respect and protect the freedom of expression of users by seeking to avoid and minimize the impact of government restrictions,"[141] the Implementation Guidelines give specific content to this obligation—companies must interpret restrictions narrowly and challenge them where inconsistent with in-

135. Press Release, Office of Sen. Dick Durbin, Durbin Statement of Final Approval on Long Awaited Internet Code of Conduct (Oct. 28, 2008), *available at* http://durbin.senate.gov/showRelease.cfm?releaseId=304621.

136. Commission Proposal for a Directive of the European Parliament and of the Council Concerning the EU Global Online Freedom Act, COM (2008), available at http://www.julesmaaten.eu/_uploads/EU%20GOFA.htm (last visited March 1, 2009).

137. Press Release, Global Network Initiative, *supra* note 27.

138. GLOBAL NETWORK INITIATIVE, PRINCIPLES ON FREEDOM OF EXPRESSION AND PRIVACY, *available at* http://www.globalnetworkinitiative.org/cms/uploads/1/GNI_-_Principles_1_.pdf (last visited Dec.19, 2008).

139. *See supra* Section I.B.1.

140. GLOBAL NETWORK INITIATIVE, IMPLEMENTATION GUIDELINES FOR THE PRINCIPLES ON FREEDOM OF EXPRESSION AND PRIVACY, *available at* http://www.globalnetworkinitiative.org/cms/uploads/1/GNI_-_Implementation_Guidelines_1_.pdf (last visited Dec. 19, 2008).

141. PRINCIPLES, *supra* note 138, at 2.

ternational human rights law, for example.[142] Read together, the Principles and the Implementation Guidelines prescribe a standard of conduct for ICTs.

A third document, the Governance, Accountability and Learning Framework,[143] establishes a multi-stakeholder Organization to coordinate and advance the Initiative. Companies are to report their progress and challenges in implementing the Principles, and will ultimately be held accountable through independent assessments administered by the Organization.[144] In this regard the Organization resembles the international and regional bodies established by human rights treaties to further their implementation and enforcement. The Organization will be run by a full-time professional staff and governed by a Board equally representing company and non-company participants.[145]

The Governance, Accountability and Learning Framework lays out a three-phase roadmap to full operational capacity by 2012.[146] The first two-year phase involves capacity building for both companies and the Organization.[147] The Organization is to recruit new participants, prepare for the independent assessments of the next phase, and provide human rights expertise to participating companies.[148] Companies are to use the first phase to implement the Principles into their policies and operations.[149] Beginning in the second phase, independent assessors—appointed by companies according to criteria set by the Organization—will evaluate each company's success in implementing and operationalizing the principles.[150] In the second phase this assessment is limited to a review of policies and practices, and expands to encompass actual cases in the third phase.[151] In the later phases the Organization is to receive the concerns of both companies and interested parties and evolve the Principles as necessary.[152] At every stage, recruiting new company participants is an objective of the

142. IMPLEMENTATION GUIDELINES, *supra* note 140, at 5.

143. GLOBAL NETWORK INITIATIVE, GOVERNANCE, ACCOUNTABILITY AND LEARNING FRAMEWORK, *available at* http://www.globalnetworkinitiative.org/governanceframework/index.php (last visited Feb. 2, 2009).

144. *Id.*

145. *Id.*

146. *Id.*

147. *Id.*

148. *Id.*

149. GOVERNANCE, *supra* note 143.

150. *Id.*

151. *Id.*

152. *Id.*

Organization, and the Framework provides for the admission of new participants.[153]

1. ICT Obligations Under Global Network Initiative

The obligations of participating companies under the Global Network Initiative divide roughly into three categories. Most detailed are those duties that arise in the face of government-imposed restrictions on freedom of expression and privacy. Participating companies are also obligated to take proactive measures—to implement internal policies, governance structures and training—that enable them to fulfill the first set of obligations. This second set of obligations is less particular, leaving more discretion to the companies. Finally, participating companies commit to multi-stakeholder collaboration, such as engaging governments and cooperating in independent assessments.

The most substantial obligations arise where companies face the quandary here described: where governments demand that ICTs restrict freedom of expression and privacy. The Principles broadly state these obligations:

> Participating companies will respect and protect the freedom of expression rights of their users when confronted with government demands, laws and regulations to suppress freedom of expression, remove content or otherwise limit access to information and ideas in a manner inconsistent with internationally recognized laws and standards.[154]

An identical provision substitutes "privacy" for "freedom of expression."[155] The Implementation Guidelines give specific content to the obligation to "respect and protect" freedom of expression and privacy. When required by governments to restrict communications, remove content, or provide personal information to governmental authorities, companies commit to:

> • Require that governments follow established domestic legal processes when they are seeking to restrict freedom of expression.

153. *Id.*
154. PRINCIPLES, *supra* note 138, at 2.
155. *Id.*

> • Interpret government restrictions and demands so as to minimize the negative effect on freedom of expression.[156]
>
> • Interpret the governmental authority's jurisdiction so as to minimize the negative effect on freedom of expression.[157]
>
> [. . .]
>
> • Request clear written communications from the government that explain the legal basis for government restrictions to freedom of expression [or demand for personal information], including the name of the requesting government entity and the name, title and signature of the authorized official.
>
> [. . .]
>
> • Seek clarification or modification from authorized officials when government restrictions appear overbroad, not required by domestic law or appear inconsistent with international human rights laws and standards on freedom of expression.[158]

These obligations call for gentle-to-mildly-aggressive pushback on governmental directives that interfere with privacy and freedom of expression. Participating companies must *require* governments to explicitly justify their directives within the framework of international human rights law. That is, interferences with privacy and expression must be *prescribed by law* and *necessary* to achieve a *legitimate societal aim*.[159] Where governments fail to so justify their directives, or where justifications are not satisfactory, participating companies are obligated to respond more aggressively. In some cases they must:

> Challenge the government in domestic courts or seek the assistance of relevant government authorities, international human rights bodies or non-governmental organizations when faced with a government restriction that appears inconsistent with domestic law or procedures or international human rights laws and standards on freedom of expression.[160]

---

156. The section of the Implementation Guidelines specifically concerning *privacy* requires participating companies to "narrowly interpret and implement government demands that compromise privacy." IMPLEMENTATION GUIDELINES, *supra* note 140, at 6.

157. The Implementation Guidelines acknowledge that "the nature of jurisdiction on the Internet is a highly complex question that will be subject to shifting legal definitions and interpretations over time." *Id.* at 5.

158. *Id.*

159. *See supra* Section I.C.1.

160. IMPLEMENTATION GUIDELINES, *supra* note 140, at 5.

The Implementing Guidelines acknowledge, "it is neither practical nor desirable" to challenge every restriction, and permit companies to consider the cost and projected efficacy of a challenge in choosing their battles.[161]

In addition to obligations arising in relation to *specific* governmental directives, the Initiative obligates participating companies to "respect and protect" users' privacy and expression rights more generally. With respect to expression, this entails, "seeking to *avoid* or *minimize* the impact of government restrictions on freedom of expression."[162] One important step toward fulfilling this general obligation is for companies to free themselves from voluntary commitments to restrict free expression and privacy. The Implementation Guidelines provide:

> Participants will refrain from entering into voluntary agreements that require the participants to limit users' freedom of expression or privacy in a manner inconsistent with the Principles. Voluntary agreements entered into prior to committing to the Principles and which meet this criterion should be revoked within three years of committing to the Principles.

This provision is likely directed at the "self-discipline pact" the Chinese Information Ministry required ICTs to sign in 2002, committing ICTs "not to produce or disseminate harmful texts or news likely to jeopardise national security and social stability, violate laws and regulations, or spread false news, superstitions and obscenities."[163]

Participating companies must also "employ protections with respect to personal information in all countries where they operate in order to protect the privacy rights of others." The Implementation Guidelines elaborate:

> Participating companies will assess the human rights risks associated with the collection, storage, and retention of personal information in the jurisdictions where they operate and develop appropriate mitigation strategies to address these risks.[164]

---

161. *Id.*

It is recognized that it is neither practical nor desirable for participating companies to challenge in all cases. Rather, participating companies may select cases based on a range of criteria such as the potential beneficial impact on freedom of expression, the likelihood of success, the severity of the case, cost, the representativeness of the case and whether the case is part of a larger trend.

Id.

162. PRINCIPLES, *supra* note 138, at 2 (emphasis added).

163. Reporters without Borders, *supra* note 15, at 1 (quotations omitted).

164. IMPLEMENTATION GUIDELINES, *supra* note 140, at 6.

This obligation appears vague compared to company obligations relating to specific governmental directives and leaves almost total discretion to companies as to its implementation. At least one participant has suggested that there would be little value in providing greater specificity—for example, by limiting where servers may be located—because such rules would quickly become irrelevant given the rapid pace of technological change.[165]

One of the more challenging realities addressed by the Initiative is that U.S. ICTs frequently do business in Internet restricting countries with and through local business partners and subsidiaries whose operations affect the freedom of expression and privacy. For example, Yahoo! holds a 40% stake in leading Chinese ICT Alibaba.com, and Yahoo! CEO Jerry Yang[166] occupies a seat on Alibaba's four-person board.[167] Skype partners with Chinese ICT TOM Online, which was recently discovered to have logged user information and text messages concerning sensitive subjects on an unsecured server in China.[168] The Initiative accordingly obligates participating companies to facilitate implementation of the Principles by their business partners and subsidiaries.

> Participating companies will implement these Principles wherever they have operational control. When they do not have operational control, participating companies will use best efforts to ensure that business partners, investments, suppliers, distributors and other relevant related parties follow these Principles.[169]

This sets up two tiers of responsibility: participating companies are responsible for *implementing* the Principles wherever they have "operational

---

165. *See* Geoffrey Fowler, *Parsing the Google, Yahoo, Microsoft "Global Network Initiative*, W.S.J. CHINA JOURNAL, Oct. 28, 2008, http://blogs.wsj.com/chinajournal/2008/10/28/parsing-the-google-yahoo-microsoft-global-network-initiative/trackback/ (last visited Nov. 2, 2008) (suggesting that the rapid pace of technological development motivated the vagueness of some obligations).

166. Jerry Yang resigned as CEO of Yahoo! Inc. on November 17, 2008, and, at time of writing, it is unclear who will occupy his seat on the Alibaba board. Brad Stone and Claire Cane Miller, *Jerry Yang, Yahoo Chief, Steps Down*, N.Y. TIMES., Nov. 17, 2008, at B1.

167. Press Release, Yahoo! Inc., Yahoo! And Alibaba.com Form Strategic Partnership In China (Aug. 11, 2005), *available at* http://docs.yahoo.com/docs/pr/release1256.html (last visited Nov. 12, 2008).

168. John Markhoff, *Skype Text is Monitored in China*, N.Y. Times, Oct. 2, 2008, at C1; Nart Villeneuve, Breaching the Trust: An analysis of surveillance and security practices on China's TOM-Skype platform, a joint report of *Information Warfare Monitor* and *ONI Asia*, (2008), http://www.infowarmonitor.net/breach ingtrust.pdf.

169. PRINCIPLES, *supra* note 138, at 3.

control," but have a less outcome-oriented obligation to use "best efforts" where they do not. "Operational control," the trigger of the duty to implement the Principles, is defined as:

> [T]he power, directly or indirectly, to direct or cause the direction of the management and policies of the entity. This may be by contract, ownership of voting stock or representation on the Board of Directors or similar governing body.[170]

"Best efforts" is defined as:

> The participating company will, in good faith, undertake reasonable steps to achieve the best result in the circumstances and carry the process to its logical conclusion.[171]

ICT commitments under the Initiative extend not only to the companies' relationships with governments, but with users as well. Participating companies are obligated to communicate to their users the instances in which they restrict access to Internet content as well as their policies for retention and provision of personal information to governmental authorities. More specifically, companies must disclose the laws that require them to restrict content, the companies' policies and procedures for responding to government demands to restrict or remove content, and to:

> Give clear, prominent and timely notice to users when access to specific content has been removed or blocked by the participating company or when communications have been limited by the participating company due to government restrictions. Notice should include the reason for the action and state on whose authority the action was taken.[172]

Participating companies must likewise disclose to users what *personal information* they collect, the laws and policies that may require them to provide this information to government authorities, and the companies' policies and procedures for responding to such governmental demands.[173]

Finally, the Implementation Guidelines prescribe internal measures participating companies should take to enable them to fulfill their primary obligation to safeguard free expression and privacy. Boards and senior management of participating companies are to incorporate the human rights impact assessments in reviewing company operations, evaluating

---

170. *Id.* at 5, n.10.
171. *Id.* Annex A.
172. IMPLEMENTATION GUIDELINES, *supra* note 140, at 6.
173. Id. at 7.

potential markets, as well existing and potential partners, suppliers and investors.[174] Companies are to:

> Adopt policies and procedures to address how the company will respond in instances when governments fail to provide a written directive or adhere to domestic legal procedure. These policies and procedures shall include a consideration of when to challenge such government demands.[175]

Government demands implicating users' freedom of expression and privacy are to be "overseen and signed-off by an appropriate and sufficiently senior member of the company's management."[176] And companies are to provide training to employees at all levels—including employees of partners where "appropriate and feasible"—in the companies' policies and procedures for protecting free expression and privacy.[177]

2. Accountability for Obligations Under Global Network Initiative

Accountability for compliance with the Principles is accomplished through a process of independent assessments.[178] Informed by company reporting and their own investigation, independent assessors will evaluate each company's compliance with the Principles.[179] A public determination will ultimately be made as to whether or not the companies are in compliance with their obligations.[180]

The accountability mechanism will progress in three phases over the next four years. Participating companies are given until 2011 to implement the Principles, and are subject to no assessment until this time. During this first phase, the Board of the Organization is to approve independence and competence criteria for the selection of independent assessors.

In the second phase, commencing in 2011, independent assessments of company *processes* will be conducted. Each company will select one or several independent assessors who meet the Board's criteria for independence and competence. The first round of independent assessments will take the following form:

> To initiate the independent assessment, each company will prepare a detailed report describing its internal processes that im-

174. *Id.* at 1-2.
175. *Id.* at 5.
176. *Id.* at 3.
177. *Id.* at 4.
178. *See* GOVERNANCE, *supra* note 143, at 2-3.
179. *Id*. at 3-4.
180. *Id*. at 3-5.

> plement the Principles. The independent assessors will review the company's report as a baseline and also review the companies' internal implementation processes in operation. Based on these reviews the independent assessors will prepare a written evaluation of the company's internal processes that implement the Principles.[181]

In addition to their reporting obligations, companies agree to provide sufficient access to enable independent assessors to perform their own investigation.[182] It bears emphasis that this first assessment in 2011 and the companies' reporting leading to it will be limited to *process*: whether participating companies have implemented the Principles in their operations as required by the Principles and Implementation Guidelines. It is unclear from the Governance, Accountability and Learning Framework whether the results of this first assessment—the verdict of whether or not individual companies are in compliance with the Principles—will be made public.[183]

The accountability mechanism comes fully into effect in the third phase.[184] The scope of company reporting and independent assessments expands to include actual cases—company responses to specific government demands—and the effectiveness of company responses. Independent assessors are also permitted to consider information brought to their attention by third parties at this stage, creating a possible role for NGOs in the assessments.[185] From these assessments, the Board of the Organization will *publicly* determine whether each company is in compliance with the Principles.[186]

3. Civil Society Reception of the Global Network Initiative

The civil society participants in the Global Network Initiative reacted with cautious optimism to the Initiative's launch.[187] The sentiment of NGO participants is aptly captured by the reaction of Human Rights

---

181. *Id*. at 3.

182. *Id.*

183. The Framework does specify "the Organization will produce a report outlining its activities during the year, including a *description* of the independent assessment process." *Id.* at 4 (emphasis added). When compared to the description of Phase 3—where, under the Independent Assessment heading, it is explicitly stated that the determination will be made public—it appears there will be no public determination until 2012.

184. At this time the Organization will accredit a pool of qualified Independent Assessors. *See id.* at 4-6.

185. *Id.* at 4.

186. *Id.*

187. Global Network Initiative, *supra* note 137.

Watch. "This initiative is an important opportunity to ensure respect for human rights in the ICT industry. The hard work is still ahead, but this is an important step forward."[188] However, two major human rights NGOs that participated in the two-year gestation of the Initiative distanced themselves just before its unveiling, contending that it does not go far enough. Amnesty International issued a statement recognizing the progress of the Initiative, but concluding that it is "not yet strong enough for Amnesty International to endorse."[189] Reporters Without Borders cited "loopholes" and "weak language on the central points" as the reason for its withdrawal of official support.[190] More specifically, it criticized the absence of an outright prohibition on ICT compliance with repressive local laws, stating that "[u]nder these principles, another Shi Tao case is still possible."[191] It also criticized the extent of discretion left to companies—such as when they will challenge government demands—and the possibility that participating companies will skirt their obligations under the Initiative through local business partnerships.[192]

B. Assessing The Global Network Initiative

The Global Network Initiative is a positive step toward alleviating the quandary facing ICTs operating in Internet-restricting countries. It should be evident from Part I that ICTs simply cannot afford to acquiesce, as a matter of policy, to repressive local regulations that breach the global law to which they are simultaneously accountable. The Initiative helps companies to comply with this global law to the maximum extent possible, first by distilling vast bodies of international human rights law into relatively concrete, actionable obligations that can be incorporated into company policies and operations. The Initiative is also structured to enable collective action where individual action would be impracticable by creating a so-called "cartel of values"[193] among participating companies. It should

---

188. Arvind Ganesan, Director, Business and Human Rights Program, Human Rights Watch, quoted in Oct. 28, 2008 press release, *supra* note 137.

189. Bobble Johnson, *Amnesty Criticises Global Network Initiative for Online Freedom of Speech*, GUARDIAN, Oct. 30, 2008, *available at* http://www.guardian.co.uk /technology/2008/oct/30/amnesty-global-network-initiative.

190. Reporters Without Borders for Press Freedom, "Why Reporters Without Borders is not endorsing the Global Principles on Freedom of Expression and Privacy for ICT companies operating in Internet-restricting countries" (Oct. 28, 2008) http://www.rsf.org/print.php3?id_article=29117.

191. *Id.*

192. *Id.*

193. Ralph Steinhardt, *Corporate Responsibility and the International Law of Human Rights: The New* Lex Mercatoria, *in* NON-STATE ACTORS AND HUMAN RIGHTS 202-203 (Philip Alston ed., 2005).

enable greater resistance by ICTs by overcoming two collective action problems: if all participating companies adhere to obligations, none should suffer competitive disadvantages vis-à-vis each other, and the unified front brings greater market power to bear on governments.

But Human Rights Watch was correct to observe that the hard work lies ahead. This hard work is the implementation and operationalization of the Principles by participating companies, and diplomatic engagement with Internet-restricting countries. The Principles will be little more than a public relations exercise if not faithfully implemented by participating companies, and meaningfully enforced by the Organization. Critics of the Principles are correct that they leave much discretion to companies as to the *means* of fulfilling key obligations. Yet concerns that this discretion amounts to "loopholes" may be premature. Independent assessments, properly conducted, can correct for any "play" in the rules. The obligations contained in the Principles and Implementation Guidelines should not be read in isolation but, like a statute or treaty, construed in light of their object and purpose—articulated in the Preamble and high-level obligations—and the body of international human rights law incorporated by reference. Approached in this way, companies that act contrary to the *spirit* of the Principles cannot escape the scrutiny of independent assessors by relying on vague or "optional" language. The Principles, together with the Implementation Guidelines and the international human rights law underlying both, provide sufficient standards to assess whether participating companies have in good faith met their *overall* obligations to respect and protect the freedom of expression and privacy. If participating companies are able to exploit vague or discretionary provisions to evade their obligations, it will be a failure not of the Principles, but the independent assessors.

Faithfully implemented and enforced, the upside potential of the Initiative is to press the protection of free expression and privacy to the limits of private action. Even Google, Yahoo! and Microsoft, standing shoulder to shoulder under the Initiative, do not likely possess the market power to flatly refuse all cooperation with the Chinese government.[194] Yet it is

194. In pursuit of a durable solution to this quandary, Google has requested that the U.S. government treat Internet censorship as a trade barrier. Posting by Andrew McLaughlin, Google Public Policy Blog, http://googlepublicpolicy.blogspot.com/2007/06/censorship-as-trade-barrier.html (June 22, 2007, 15:36 PST). Taking a similar tack, the European Parliament has passed a resolution calling on the European Union to treat Internet censorship as a trade barrier. European Parliament resolution of 19 February 2008 on the EU's Strategy to deliver market access for European companies, EUR. PARL.

equally likely that the companies have not reached the limit of their power to push back on demands to restrict free expression and privacy—by interpreting restrictions narrowly and requiring governments to justify demands according to international human rights standards, for example. At best, the Initiative can enable ICTs to recover this lost ground between their present practices and the full extent of their private potential to resist governmental directives inconsistent with human rights.

Two recent incidents of state-mandated interference with expression and privacy illustrate the means available to ICTs to mitigate such interferences, the limits of private action, and the varying willingness of leading ICTs to explore this limit. In the United States, Google successfully challenged a subpoena[195] for millions of user search queries. The Department of Justice subpoenaed leading U.S. search engines for samplings of search terms and URLs to aid its prosecutions under the Child Online Protection Act of 1998.[196] Whereas America Online, Yahoo! and MSN reportedly complied with the subpoena,[197] Google challenged the subpoena, persuading the District Court for the Northern District of California to narrow the disclosure mandate to eliminate user search queries.[198]

In Argentina, numerous public figures have secured temporary restraining orders against Yahoo! Argentina and Google Argentina to block search results containing their names.[199] Both Yahoo! and Google challenged the restraining orders in Argentinean courts, but have implemented them differently, according to the OpenNet Initiative.[200] Whereas Yahoo! Argentina eliminated *all search results* for individual celebrity names and did not provide notice of filtering to users until November 10, 2008, Google Argentina implemented the orders more narrowly and consistently provided notice to users that search results were limited by court order.[201]

DOC. (2007/2185(INI)), *available at* http://www.europarl.europa.eu/sides/getDoc.do?type=TA&language=EN&reference=P6-TA-2008-0053.

195. Subpoena Duces Tecum, ACLU v. Gonzales, No. 98-5591 (Ed. Pa. Aug. 25, 2005), *available at* http://www.google.com/press/images/subpoena_20060317.pdf.

196. Katie Hafner and Matt Richtel, *Google Resists U.S. Subpoena of Search Data*, N.Y. TIMES, January 20, 2006, at A1.

197. *Id.*

198. Order Granting In Part And Denying In Part Motion To Compel Compliance With Subpoena Duces Tecum, Gonzales v. Google, Inc., No. CV 06-8006, (N.D. Cal. Mar. 17, 2006).

199. Firuzeh Shokooh Valle and Chistopher Soghoian, *Adios Diego: Argentine Judges Cleanse the Internet*, OpenNet Initaitive Blog, Nov. 11, 2008, http://opennet.net/blog/2008/11/adiós-diego-argentine-judges-cleanse-internet (last visited Nov. 29, 2008).

200. *Id.*

201. *Id.*

Although the court orders ultimately led to far-reaching Internet censorship, the pushback by the ICTs—court challenges, narrow interpretation, and transparency to users—resulted in *less* interference with expression than unquestioning compliance with government commands.

The Globlal Network Initiative provides for the type of private resistance undertaken by Google and Yahoo! in the U.S. and Argentina, but with the advantages of coordination and uniformity. Uniform responses to government demands, absent in the above examples, may be achieved through the uniformity of participants' obligations under the Initiative, and the potential for the Organization to facilitate information sharing among otherwise fierce competitors, formulating coordinated responses to shared problems. Such a uniform approach to government-imposed restrictions on free expression and privacy by the present participants may even drive market-based convergence around this approach by non-participants. Such market-driven convergence is presently playing out as Yahoo!, Google, Microsoft, and Ask.com race to outdo one another in adopting more privacy-oriented practices for handling user data, competing for the user trust that is crucial to brand value.[202] A uniform approach by three leading ICTs may spark similar competition.

Would a Shi Tao case still be possible under the Global Network Initiative, as Reporters Without Borders has cautioned?[203] Perhaps. Private ICTs do not have the power to completely resist demands for information a government is determined to obtain. But in resisting to the limits of private action as prescribed by the Principles, ICTs raise the cost for governments of obtaining information contrary to human rights norms, and the cost of imposing restrictions on expression and privacy more generally. We cannot know whether the Shi Tao tragedy would have been averted using the means of private resistance prescribed by the Global Network Initiative; we know only that such tragedies have occurred, and continue to occur,[204] under prevailing ICT policies.

---

202. *See, e.g.*, Nate Anderson, *Yahoo Outdoes Google, Will Scrub Search Logs After 90 Days*, ARS TECHNICA, Dec. 17, 2008, http://arstechnica.com/news.ars/post/20081217-yahoo-outdoes-google-will-scrub-search-logs-after-90-days.html (last visited Dec. 18, 2008).

203. Reporters Without Borders, *supra* note 190.

204. In February 2008, Yahoo! was again sued under the ATCA for aiding and abetting the persecution of Chinese dissidents by furnishing the Chinese government with user-identifying information. Complaint, Cunzhu et al v. Yahoo! Inc. et al, No. C08-01068 (N.D. Cal. Feb. 22, 2008), *available at* http://docs.justia.com/cases/federal/district-courts/california/candce/3:2008cv01068/200778/1/ (last visited Mar. 1, 2009).

In any case, to dismiss the Global Network Initiative as futile for its inability to resolve the most difficult cases would be shortsighted. Short of wholesale defiance of sovereign commands, many opportunities for valuable improvement of Internet freedom remain squarely within reach for private actors. Just as ICT resistance *mitigated* the adverse effect of the Argentinean court orders on free expression, ICTs—guided by the Principles of the Global Network Initiative and the creativity that has defined their success—have the potential to incrementally improve free expression and privacy *everywhere* they operate by questioning, challenging, and narrowing repressive regulations. In providing a roadmap and support apparatus for compliance with the global law, the Global Network Initiative offers ICTs the best available solution to both moral and business quandaries.