



September 30, 2008

Dr. Hamadoun I. Touré
Secretary-General
International Telecommunication Union
Place des Nations
1211 Geneva 20
Switzerland

Dear Dr. Secretary-General,

We are writing to express our concern regarding the International Telecommunication Union-Standardization's (ITU-T) decision to draft technical standards for tracking the source of Internet communications without input from civil society organizations. According to news reports, the ITU has initiated a process "to define methods of tracing the original source of Internet communications and potentially curbing the ability of users to remain anonymous."¹

This effort is being lead by the "IP Traceback" drafting group, named Q6/17. This drafting group consists of representatives from the United States National Security Agency, the Chinese government and industry, but does not include representation from the civil liberties or human rights communities. This is unacceptable. The creation of fundamental standards of Internet architecture cannot be left to the intelligence community and repressive regimes.

The drafting group has also refused to conduct itself in the open and transparent manner that is expected of international institutions. It has refused to release key documents regarding the program or open meetings to the public. As a result unaccountable institutions within a closed forum are leading this policy.

Our concern about this group's activities is magnified by the fact that one of the reported goals of the Q6/17 group may be to stifle political dissent by identifying dissidents and eliminating anonymity for political speech.² The purpose of this IP trace-back effort would be to enable any IP packet to be traced backward to its origin. We understand that the ITU would see a number of desirable outcomes from such a trace-back including the reduction of distributed denial of service attacks, the enhancement of anti-virus security, and the reduction of anonymous Internet threats.

However no matter what possible benefits the proposal might have, it is certain that the creation and implementation of such a standard would have much greater negative effects on free speech and privacy on the Internet. Any attempt to impose them would almost certainly be illegal, running afoul of the US Constitution and free speech rights.

Free Speech

Free expression is protected under Article 19 of the Universal Declaration of Human

¹ Declan McCullagh, *U.N. agency eyes curbs on Internet anonymity*, CNET NEWS, September 12, 2008.

² *Id.*

AMERICAN CIVIL LIBERTIES UNION

TECHNOLOGY AND LIBERTY PROGRAM

PLEASE RESPOND TO:
WASHINGTON, DC OFFICE
915 15TH STREET, NW, 6TH FL.
WASHINGTON, DC 20005
T/202.544.1681
F/202.546.0738
WWW.ACLU.ORG

NATIONAL OFFICE
125 BROAD STREET, 18TH FL.
NEW YORK, NY 10004-2400
T/212.549.2500
F/212.549.2629

OFFICERS AND DIRECTORS

NADINE STROSSEN
PRESIDENT

ANTHONY D. ROMERO
EXECUTIVE DIRECTOR

KENNETH B. CLARK
CHAIR, NATIONAL
ADVISORY COUNCIL

RICHARD ZACKS
TREASURER

Rights. Many regional human rights instruments elaborate on this right, for instance under Article 10 of the European Convention on Human Rights.

National constitutions also protect this right as it is seen as essential for the protection of democratic life. In Europe, for instance, it is seen as essential protection for journalists. In the case of *Goodwin v. The United Kingdom*, the European Court of Human Rights recognised that the role of the press as a watchdog in a healthy democratic society can be undermined if journalists were compelled to disclose information about their sources.³ Yet this is the very same information that would be made available through IP trace-back.

Free and anonymous speech is one of the core guarantees of the First Amendment to the US Constitution. The US has a long history of engaging in anonymous speech for political purposes and one of the central documents used to interpret the Constitution is the *Federalist Papers*, written by the US founding fathers but published anonymously.⁴

Any IP trace-back proposal would have a chilling effect on this protected speech. The purpose of anonymous speech in US law is clear:

Under our Constitution, anonymous pamphleteering is not a pernicious, fraudulent practice, but an honorable tradition of advocacy and of dissent. Anonymity is a shield from the tyranny of the majority. ... It thus exemplifies the purpose behind the Bill of Rights, and of the First Amendment in particular: to protect unpopular individuals from retaliation-and their ideas from suppression-at the hand of an intolerant society.⁵

There is no question that under US law this protection on anonymous speech extends to Internet communications.⁶ The group's activities fail to acknowledge this essential and widely recognised right, and importantly its implications for individual privacy.

Privacy

Privacy is also protected under international conventions and norms. Article 12 of the Universal Declaration of Human Rights calls for the protection of privacy, as does Article 17 of the International Covenant on Civil and Political Rights (ICCPR), and Article 16 of the UN Convention on Protection of the Child. This right is also protected under regional instruments, such as in Article 8 of the European Convention on Human Rights, and Article 11 of the American Convention on Human Rights. Most countries also implement thorough legal protections in their constitutions and in statute.

In the United States, it is a long held Constitutional doctrine that the search and seizure provision of the Constitution protects people from unwarranted surveillance.⁷ In turn, an individual's privacy is protected under US law, including their web surfing

3 Article 19, Background Paper on Freedom of Expression and Internet Regulation for the International Seminar on Promoting Freedom of Expression With the Three Specialised International Mandates, London, United Kingdom, 19-20 November 2001.

4 See *McIntyre v. Ohio Elections Commission*, 514 U.S., at 343.

5 *McIntyre* at 357.

6 See, for instance, *American Civil Liberties Union of Georgia v. Miller*, 977 F. Supp. 1228 (N.D. Ga. 1997).

7 *Katz v. United States*, 389 U.S. 347.

habits. For example, in *State v. Reid*,⁸ the court protected the privacy of subscriber information and emphasized the importance of Internet privacy, “[t]he government can learn the names of stores at which a person shops, the political organizations a person finds interesting, a person's ... fantasies, her health concerns, and so on.”⁹

Any effort to pierce this privacy shield will face significant legal hurdles under both international and US law. The ITU should not act as that piercing mechanism, and if it is considering doing so it must open itself up to allow for careful consideration on this pressing issue.

Transparency

In recent years we have seen many of the most closed international organisations open their doors in order to enhance transparency for policy deliberation. Consistent with the spirit of the World Summit on the Information Society and the practices increasingly common elsewhere in the United Nations system, work on security should be opened.

In fact, paragraph 52 of the WSIS Tunis Agenda states:

“In order to ensure effective participation in global Internet governance, we urge international Organisations, including inter-governmental Organisations, where relevant, to ensure that all stakeholders, particularly from developing countries, have the opportunity to participate in policy decision-making relating to Internet Governance, and to promote and facilitate such participation.”¹⁰

We are thus alarmed by the closed nature of these discussions on matters of such importance. Nearly every policy process dealing with Internet security has been subject to open processes and we are amazed that the ITU insists on being the exception to this emerging rule.

Further, the Joint Declaration signed by the United Nations Special Rapporteur on Freedom of Opinion and Expression noted that international institutions have an obligation to be transparent and provide access to the information they hold.¹¹ Additionally the Special Rapporteur:

[V]igorously emphasizes that any new intergovernmental body administering, partially or totally, Internet governance must be anchored in a human rights vision. The universality of the right to freedom of opinion and expression, as defined in article 19 of the Universal Declaration of Human Rights, and reiterated in other human rights instruments like the International Covenant on Civil and Political Rights, the African Charter on Human and Peoples’ Rights, the American Convention on Human Rights and the European Convention for the Protection of

⁸ 194 N.J. 386, 945 A.2d 26 (N.J. 2008).

⁹ *Reid* at 398.

¹⁰ WSIS, Tunis Agenda for the Information Society, available at <http://www.itu.int/wsis/docs2/tunis/off/6rev1.html>. Paragraphs 60 to 62 have similar statements about transparency and participation.

¹¹ International Mechanisms for Promoting Freedom of Expression, A Joint Declaration by the UN Special Rapporteur on Freedom of Opinion and Expression, the OSCE Representative on Freedom of the Media, the OAS Special Rapporteur on Freedom of Expression and the African Commission on Human and Peoples’ Rights Special Rapporteur on Freedom of Expression, December 2006.

Human Rights and Fundamental Freedoms should guide Governments and the international community at large in this endeavour." 12

Ultimately the ITU has a duty to conduct its proceedings in an open and transparent manner and to respect human rights and fundamental freedoms.

What the ITU should do

The ITU must ensure openness and transparency in the standards setting process and conduct a thorough evaluation of any IP trace-back proposals. Current descriptions of the project are opaque and worse seem to implicate political speech.

Specifically we ask the ITU to:

- To consider alternatives to IP trace-back for improving Internet security and operation;
- Release all documents surrounding the IP trace-back group's activities so they can be evaluated by external observers and experts;
- Open membership in Q6/17 to experts and observers including members from civil society organisations, and in particular from civil liberties and human rights groups.

In short anonymity is not a problem to be solved, but rather an affirmative good. From the benefits of the secret ballot to its utility in allowing for the exposure of government wrongdoing, anonymous speech and activity actively benefit society. While we hope that the ITU's efforts to create standards for IP trace-back have been driven by a sincere effort to protect Internet security, if the end result of this effort is the elimination of true anonymity and privacy on the Internet, we fear that the cure is worse than the disease.

Sincerely,



Barry Steinhardt
Director, ACLU Technology & Liberty Program



Gus Hosein
Senior Fellow, Privacy International

Cc: Ms. Navi Pillay
UN High Commissioner for Human Rights