Welcome to the World of Human Rights: Please Make Yourself Uncomfortable

Henry Corrigan-Gibbs and Bryan Ford
Yale University
New Haven, Connecticut, U.S.A.
Email: {henry.corrigan-gibbs, bryan.ford}@yale.edu

***Abstract*—We draw an ethical analogy between Internet freedom efforts and humanitarian aid work. This parallel motivates a number of ethical questions relating to anonymity and censorship-circumvention research.**

***Keywords*-ethics; censorship; circumvention; anonymity; human rights; humanitarian**

I. Introduction

The proliferation of firewalling, anonymity, and censorship-circumvention tools gives computer scientists a growing role in creating and circumventing Internet access controls. Yet, even as computer scientists take the lead in deploying these technologies in armed conflict zones (e.g., Syria) and in countries with large-scale Internet censorship regimes (e.g., China), there has been a notable dearth of debate in the computer science community about the ethical questions surrounding these interventions. A few example scenarios demonstrate the ethical quandaries that Internet freedom work raises:

1) A computer scientist who works on censorship-circumvention tools gets an email from a rebel fighter in Syria who asks for help in bypassing the Syrian government firewall. Under what circumstances, if any, should the researcher offer his technical assistance to the rebel?
2) An undergraduate computer science major is preparing to enter the job market. After submitting a batch of applications, she receives a financially attractive job offer from a company that manufactures deep packet inspection firewalls. She knows that this company sells their products to American corporations but that they also sell firewalls to Bahrain (a country that censors the Internet). Should she take the job?
3) A computer science researcher running an experimental anonymizing Web proxy discovers that more than half of the proxy's users are using it to cloak illegal activities, though many users are just using the service to anonymize their innocuous browsing sessions. Should the researcher keep the service running?

One reason for the lack of debate over these issues may be the increasingly common opinion that unrestricted and untraceable access to the global Internet is a *human right*, and is therefore an unequivocal good. Experiences from a community well-versed in human rights promotion—the humanitarian aid community[1]—contradict this simplistic view. Indeed, the humanitarian aid community has long struggled with the many ethical dilemmas that arise when promoting human rights around the world.

We argue that the Internet freedom community should use the experiences of the humanitarian aid community to stimulate and inform a debate over the ethics of Internet freedom research. By drawing on the extensive literature and lessons on the ethics of humanitarian aid interventions, computer scientists and technology policy-makers can avoid repeating the mistakes of failed humanitarian interventions and can better evaluate the morality of their own actions.

II. Internet Access as a Right

Activists and civic leaders have used the Universal Declaration of Human Rights, adopted by the UN General Assembly in 1948, as a rallying point for their beliefs in Internet freedom. Article 19 of the Declaration states:

> Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers. [2]

The home page of torservers.net prominently quotes the Declaration, U.S. Secretary of State Hillary Clinton cited it in her much-publicized speech on Internet freedom [3], and a report of the American Association for the Advancement of Science (AAAS) points to the the Declaration as evidence that anonymous communication "should be regarded as a strong human right" [4].

Furthermore, the international community, as represented through the Millennium Development Goals process, has designated Internet access as a human development objective, on par with eliminating HIV/AIDS, reducing child mortality rates, and achieving universal primary education [5,

[1] Kieran Donaghue notes that organizations "dedicated to securing the vital interests of vulnerable human beings" are often divided into the categories of human rights groups, humanitarian groups, and development-focused groups [1, p. 39]. We use the term "humanitarian aid" groups loosely to refer to all three classes of organization.

pp. 63–65]. Naturally, each of these sources defines "Internet freedom" and "Internet access" in a manner that serves their own political or economic interests. Notwithstanding the debate over definitions, many important international actors regard access to the global Internet (however defined) as a human right and a key human development objective.

Accepting the position that Internet access is a human right does not provide satisfactory answers to all of the important ethical questions about Internet freedom. For example, a facile argument states that since private Internet access is a human right, training Internet users on how to use an anonymizing proxy is *always* a good thing. Yet, it somehow seems ethically wrong to teach agents of a repressive state's secret police to use an anonymizing proxy to conceal their snooping. Even so, the human rights of these agents—the right to Internet access, in particular—are as valuable as the human rights of any other person. How can we reconcile the moral imperative to extend the right of Internet access to *all* humans with the natural instinct to prioritize our work to help some groups of people (e.g., citizens in China) before others (e.g., the Syrian secret police)?

III. Lessons from Humanitarian Aid

The fundamental question—when and how to intervene to help promote the human rights of a population—is not a new one. Indeed, humanitarian organizations have struggled with this problem for decades. Entire journals, such as *Ethics & International Affairs*, are dedicated to studying the relationship between "principles of justice and morality" and the "conduct of important international actors" [6]. Computer scientists can draw on the humanitarian aid community's decades of experience and intense ethical soul-searching to help inform ourselves about the questions we face about the ethics of promoting Internet freedom.

In the following sections, we present a handful of ethical issues that humanitarian aid work has raised and we discuss the lessons that these debates may offer to the Internet freedom community.

Lesson 1: Impartiality is Impossible

The first lesson that computer scientists should draw from the humanitarian aid community is that as soon as an organization enters a conflict zone (for the purpose of providing food, shelter, or even Internet access), it risks becoming a party to that conflict.

For many years, the dominant opinion in the humanitarian community was that "humanitarian action can and should be completely isolated from politics" [7, p. 2]. Distributing food, water, and shelter—the thinking went—was an apolitical act, so aid organizations should operate without entangling themselves in messy political conflicts. Some organizations in the Internet freedom community implicitly take a similar position today: uncensored and private Internet access is a human right, so it is possible to promote circumvention and anonymity tools independently of an area's local political environment.

Since the end of the Cold War, however, many humanitarian organizations have found that it is impossible or untenable to stay completely neutral in conflict zones [7]. Post-genocide Rwanda offers a particularly painful example of how the apolitical promotion of human rights can have disastrous effects. In that conflict, ostensibly independent humanitarian aid organizations provided the food and supplies that inadvertently sustained a genocidal government-in-exile [8, pp. 313–315]. Organizations that entered the refugee camps with the goal of impartiality and independence ended up helping one side in the conflict by default.

Today's Internet freedom organizations are vulnerable to falling into the same ethical trap that snared aid organizations after the Rwandan genocide. Internet freedom organizations that provide tools and trainings to activists, bloggers, and civil society activists must appreciate that *who* they are teaching is as important as *what* they are teaching. Giving trainings and Internet freedom tools to a group of people is, in essence, furthering that group's political agenda over the agendas of competing groups.

Training one group of dissidents on how to use censorship-circumvention tools gives that group a technological advantage over other dissidents vying for power. Training pro-democracy bloggers who have radically anti-feminist views could harm women's rights in a country in the long run. While the real-world effects of Internet safety trainings offered by civil society groups are much more subtle than these examples suggest, these trainings *do* have consequences for the relative balance of power between groups.

The lesson to draw from the humanitarian community's experience is that organizations should carefully consider who they are helping and what impact that their training and tools will have, rather than hiding behind the false shield of impartiality.

Lesson 2: It's Hard to Consent When You Don't Understand

Another lesson drawn from the humanitarian aid community is that if a user does not understand the costs, benefits, abilities, and limitations of a particular tool, then advising them to use it is ethically questionable.

Luise White uses the story of a 1960s smallpox vaccination campaign in East Africa to discuss this problem of informed consent [9]. During the course of the campaign, a medical advisor observed that health workers were administering three-month-old smallpox vaccines, even though the vaccine was only effective for a day or two after its manufacture. In addition, patients who lined up to receive the vaccination came with "coughs and aches and travel plans," apparently expecting that the vaccine would cure the

common cold, relieve their muscle pain, and prevent bad luck on the road [9, pp. 456–457].

White uses this story as a means to argue that the concept of smallpox as a global health concern "originates so far from African concerns and African consent that [the campaign] cannot be called ethical at all" [9, p. 458]. If the clinicians did not have the training to understand that the vaccines had expired, and the patients had unrealistic expectations of the vaccine's benefits, then it is difficult to argue that the patients were able to truly consent to the treatment.

The line of expectant patients waiting for their good-luck immunization is reminiscent of Internet users who are vaguely aware of the benefits of Internet privacy tools, but lack the technical knowledge to use them properly. For example, BitTorrent traffic comprised an estimated 40% of the bytes transferred over the Tor anonymity network in 2008 [10], yet the design of the BitTorrent software completely undermines any anonymity that Tor might have provided [11]. Like the patients who got smallpox immunizations for good luck, BitTorrent users install Tor with the unrealistic expectation that it will somehow help them maintain their privacy.

If the users of anonymity and circumvention systems do not really understand how the technology works, is it ethical to advise them to use it? Trainers and researchers can try to explain all of the caveats associated with a particular tool or practice, just as a health worker might try to explain the nuances of the smallpox vaccine to her patients. In spite of these efforts, there will *always* be some gap, often a very significant one, in knowledge between the trainer and the trainee (and between the doctor and the patient).

Internet freedom activists and researchers must appreciate that the knowledge gap means that, when they advise users to follow a particular practice or to use a particular tool, they might be giving the user a false sense of security. In some scenarios it might be ethical to proceed without informed consent (the smallpox campaigners implicitly took this position), but activists and researchers should carefully consider the risks involved.

Lesson 3: Our Tools Promote Our Cultural Norms

Saying that a project or organization promotes or protects "human rights" implies that there is a common understanding of what a "human right" is. The existence of a *Universal* Declaration of Human Rights, rather than, say, a *Locally Interpretable* Declaration of Human Rights, supports the idea that there is a universally accepted definition of each human right.

Yet, as many members of the humanitarian aid community recognize, every government and organization has a different interpretation of human rights. The right to freedom of speech in the United States means something very different than the right to freedom of speech in Germany (where hate speech is more aggressively regulated), though the freedom of speech is enshrined in the constitution of both states [12].

Conny Lenneberg points out that an organization's interpretation of a particular human right is based as much on that organization's own cultural *values* as it is on any universal notion of human rights [13]. The act of promoting human rights in another country, then, involves (intentionally or not) the export our own cultural norms and values. Lenneberg describes how Western organizations ran "hidden" schools in Afghanistan in the 1990s to subvert the government's ban on girls' education [13, p. 200]. Operating hidden schools was an attempt to export the Western interpretation of the "right to education" (in which both boys and girls have a right to education) to Afghanistan.

In the context of Internet freedom, we must appreciate that the tools that we develop also reflect our own set of cultural values and our own interpretation of the right to freedom of expression. For example, many anonymity tools make it very easy to browse the Internet anonymously, but most do not make it easy to use file-sharing software anonymously. The design of these tools encodes a value judgement—that Internet browsing is a more important component of freedom of expression than file-sharing software is. The choices made by researchers and activists to focus on certain countries or technical problems (e.g., enabling uncensored access to news sites versus access to pornographic sites) are expressions of our own values.

The lesson to draw from Lennebergs's analysis is *not* that it is unethical to promote value-laden human rights, but that Internet freedom activists, as promoters of human rights, should "be more reflective and transparent about how far our own values influence our assessment of what is, and is not, 'consistent with the principles of basic human rights' " [13, p. 203]. Ethics requires us to be clear to ourselves, to our funders, and to our users about what values inform our interpretation of the "right to the freedom of expression."

Lesson 4: "Impact" is Elusive

The final lesson we discuss relates to how we measure the impact that Internet freedom work has on promoting human rights around the world. Humanitarian and development organizations have long struggled with this topic. Jamie Isbister begins an article on "impact" by recalling two popular questions in the Australian development sector: "What impact are you really having? [...] And how do you know?" [14, p. 147].

As Isbister discusses, coming up with satisfactory answers to these questions in the context of development or human rights work is notoriously difficult. Defining metrics for the performance of public school teachers, for example, has been the source of endless controversy [14, p. 149]. The design of the metrics often serve the interests of the funders instead of "the local communities supposedly benefitting from a program," and the wrong metrics can make failure

look like success [14, p. 151]. Even so, these questions of impact demand answers—if an organization's work has no measurable impact, then it is hard to argue that the work has an ethical basis.

The problem of measuring impact plagues the Internet freedom community in the same way it affects the humanitarian community. If the goal of researchers and activists in the community is to promote the right to access to the global Internet, is there any evidence that all of our tools, trainings, and workshops are actually furthering that goal?

The most tempting metrics to use are, of course, the simplest ones to measure: the number of daily users a system has, the number of lines of code written, or the number of research papers published about a particular system. All of these metrics are in active use today, but *none* of them answers the essential question of whether all of this work has actually increased the freedom of communication on the Internet. Every person who uses a piece of censorship-circumvention software to access a blocked Web site, does not necessarily feel *free* to speak her mind on the Internet. Every user who uses a piece of anonymity software is not necessarily *safe* from the fear that his actions online will be linked back to his real identity.

An additional concern in the Internet freedom community is that gathering data on the usage of Internet freedom technologies can compromise the very privacy and anonymity that these systems try to protect. For example, statistics on the use of a particular censorship-circumvention system might help government censors to track its users or block the system entirely. These privacy considerations make designing metrics for Internet freedom systems especially challenging.

The humanitarian aid community has engaged in a debate over how best to avoid fallacious "countable" measures of success. It would serve the Internet freedom community well to learn from that experience and to engage in a similarly rigorous examination of measurable impact.

IV. Conclusion

We do not attempt to provide answers to the moral questions raised at the start of this paper. Instead, we hope to encourage thought and discussion of the ways in which the humanitarian analogy presented herein can inform our responses to those questions.

Those of us who work on Internet freedom technologies must realize that defending human rights does not automatically put us above ethical censure. Instead, the Internet freedom community should confront the ethical issues and potential risks surrounding our work in the same way that the humanitarian aid community has confronted the ethical issues surrounding theirs. It is only by acknowledging and addressing these ethical issues that the Internet freedom community can begin to earn the moral status associated with the defense of human rights.

Acknowledgments

We thank Zeynep Tufekci for her helpful comments. This material is based upon work supported by the Defense Advanced Research Agency (DARPA) and SPAWAR Systems Center Pacific, Contract No. N66001-44 11-C-4018. Any opinions, findings and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the Defense Advanced Research Agency (DARPA) and SPAWAR Systems Center Pacific.

References

[1] K. Donaghue, "Human rights, development ingos and priorities for action," *Ethical questions and international NGOs*, pp. 39–63, 2010.

[2] U. N. G. Assembly, "The universal declaration of human rights," Resolution 217 A (III), Dec. 1948.

[3] H. R. Clinton, "Remarks on internet freedom," http://www.state.gov/secretary/rm/2010/01/135519.htm, Jan. 2010, accessed on 30/01/2013.

[4] A. Teich, M. S. Frankel, R. Kling, and Y. Lee, "Anonymous communication policies for the Internet: Results and recommendations of the AAAS conference," *Information Society*, May 1999. [Online]. Available: http://www.indiana.edu/~tisj/readers/full-text/15-2%20teich.pdf#search=%22Anonymous%20Communication%20Policies%22

[5] *The Millennium Development Goals Report*. New York: United Nations, Jun. 2012.

[6] "About — Ethics & International Affairs," http://www.ethicsandinternationalaffairs.org/about/, accessed on 24/01/2013.

[7] T. G. Weiss, "Principles, politics, and humanitarian action," *Ethics & International Affairs*, vol. 13, no. 1, Apr. 2006.

[8] G. Prunier, *The Rwanda crisis: History of a genocide*. Columbia University Press, 1995.

[9] L. White, "Differences in medicine, differences in ethics," *Evidence, Ethos and Experiment: The Anthropology and History of Medical Research in Africa*, pp. 445–461, 2011.

[10] D. McCoy, K. Bauer, D. Grunwald, T. Kohno, and D. Sicker, "Shining light in dark places: Understanding the Tor network," in *Privacy Enhancing Technologies*. Springer, 2008, pp. 63–76.

[11] P. Manils, C. Abdelberri, S. Blond, M. Kaafar, C. Castelluccia, A. Legout, and W. Dabbous, "Compromising Tor anonymity exploiting P2P information leakage," *arXiv preprint arXiv:1004.1461*, 2010.

[12] W. Brugger, "Ban on or protection of hate speech-some observations based on German and American law," *Tul. Eur. & Civ. LF*, vol. 17, pp. 1–21, 2002.

[13] C. Lenneberg, "To respect or not to respect," *Ethical Questions and International NGOs*, pp. 193–205, 2010.

[14] J. Isbister, "Whose impact, and is it all about impact?" *Ethical Questions and International NGOs*, pp. 147–156, 2010.