HUMAN RIGHTS WATCH

The Internet is Not the Enemy

As Rights Move Online, Human Rights Standards Move with Them

By Dinah PoKempner, General Counsel

We are at a difficult juncture in the protection of online speech and privacy, when states resist applying principles they have endorsed interPnationally to their own domestic legislation and practice. It is as if all road signs to freedom of speech and privacy pointed one way, yet governments insist on taking the wrong fork, telling the alarmed passengers it is for their own safety.

Divergence between what states endorse at the United Nations and what they do at home is hardly news, though governments do not seem self-conscious when it comes to restricting rights on the internet. They seem to sense that the internet is somehow different, perhaps more powerful than older media, and reflexively reach for greater limitation.

They are right that the internet gives individuals unprecedented ability to project their communications across borders and to access the world's information. But that does not necessarily justify sacrificing privacy and speech to create unprecedented police powers.

New technology has been empowering individuals—both for good and ill—and making the world smaller for many decades, even while international human rights law grew and flourished. Typewriters may be heading towards extinction, but rights seem more important than ever. And how governments protect them in the digital age will determine whether the internet will be a force that liberates or enchains us.

What States Say and What They Do

The bifurcation between existing norms and what states really do is most evident in the unfolding debate over surveillance.

Edward Snowden, a former US government contractor, put that debate into high gear in 2013 by leaking documents to media that showed the United States and its allies were engaging in massive, indiscriminate data collection on people in the US and abroad who had no connection to wrongdoing. With the disclosures came popular and government condemnations. The UN went into high gear, with General Assembly debates and resolutions, Human Rights Council resolutions, more expert reports, and even the creation of a new expert position on privacy. Around the world, people challenged surveillance in courts and legislatures debated them.

Yet in the ensuing years, few countries curtailed surveillance powers and many instead moved to cement into their laws powers similar to what the US was shown to wield.

In the US, some reforms gained traction, though they seem unlikely to significantly curtail the breathtaking scope of data collection and real-time monitoring. Congress revised the law used to justify collecting millions of call records with another only somewhat more constraining. President Barack Obama apologized for spying on allied heads of state, but the legal authorities that undergird overseas communications surveillance still permit collection for "foreign intelligence," a vague purpose that can easily justify sweeping communications interception, including from US persons caught incidentally in the dragnet.

The United Kingdom is adopting the troubling Investigative Powers Bill, which legalizes "bulk" surveillance practices of directly tapping into undersea cables that carry internet traffic, government hacking, and thematic warrants that allow intelligence services to designate broad targets without prior judicial approval.

France also moved to place surveillance practices on a legal footing in 2015, but with deeply flawed laws, rushed through in the wake of attacks. The UN Human Rights Committee, reviewing France's compliance with the International Covenant on Civil and Political Rights (ICCPR), concluded that the intelligence law of June 2015 "grants excessively large powers of very intrusive surveillance on the basis of broad and ill-defined aims, without prior judicial authorization and without an adequate and independent oversight mechanism." Most recently, the Conseil d'Etat ruled unconstitutional the law's regime of warrantless surveillance of wireless communications.

Russia also took a retrograde path, with legislative amendments in 2016 that require companies to retain the contents of all communications for six months, data about those communications for three years, and to store all their data within Russian territory. Companies must also provide "information necessary for decoding" digital communications, a provision that may mean backdoor access to encrypted material.

China, long a leader in censoring online speech and controlling access through a national firewall, adopted a cybersecurity law in 2016 that would require companies to censor and restrict online anonymity, store user data in China, and monitor and report undefined "network security incidents," deepening fears of increased surveillance.

Even Brazil and Mexico, both critics of the mass surveillance programs of the US National Security Agency (NSA) and strong proponents of privacy at the UN, entertained cybercrime bills in 2016 that would have widened data retention requirements and constricted access to information and free speech. Germany, a leading proponent of data protection laws, approved a law in October 2016 that authorized mass untargeted surveillance of non-citizens, earning the criticism of three different UN rights experts and a legal challenge to its constitutionality.

Little wonder the UN expert on freedom of expression lamented, “One of the most disappointing aspects of the current situation … is that many States with strong histories of support for freedom of expression—in law and in their societies—have considered measures liable to abuse.”

Three Ways in which the Internet is Distinctive (and How that Scares Us)

This schizophrenic state of affairs, where states pledge allegiance to international human rights online and then legislate to curtail them, reflects a deeper split in perceptions of the internet, its promise and its peril.

There was a time when discussion of the internet and human rights rang full of utopian aspiration—the internet would set speech free, remove censoring intermediaries, enable social organizing on a scale never known. To some extent, this promise came true; activists who were stifled under authoritarian governments that suppressed organizing, protest, or an independent press could move their causes forward online. Knowledge once cabined in libraries, universities, or other networks of the elite became available to remote users in villages, fields, or slums. Minds could meet in that new location, "cyberspace," making globalized creation and impact within the reach of ordinary people.

The backlash from authorities who found this threatening was not long in coming. Dissidents and critics of illiberal governments who tried to avoid suppression by going online soon found themselves monitored, publicly shamed or arrested, a trend in full force today in Turkey, Egypt, Vietnam, Saudi Arabia, China, or Russia's Chechen Republic. Some governments, like Egypt, have even sought harsher penalties for online speech crimes than their offline counterparts.

When activists (as well as criminals) have tried to shield themselves through anonymity or encryption, governments have issued orders or proposed laws to force tech companies to hand over their users' data and decode communications. National firewalls, wholesale blocking of social media, and even internet shutdowns are used by repressive governments in efforts to control online activity.

But even in non-authoritarian settings, there is ambivalence about the internet's power of social mobilization. People may admire how democracy activists can organize online, yet worry when the Islamic State (ISIS) recruits remotely. They may applaud those who crowd source evidence of war crimes, but condemn "trolls" who expose, threaten, or harrow their victims.

To probe this growing ambivalence over the power of online speech, it is useful to consider what differentiates it from offline communication. At least three characteristics are distinctive: online speech can be more disinhibited—that is, less inhibiting—than speech in the real world; it persists and can be accessed on the internet for a long time unless deliberately removed; and it is inherently trans-border, both in the way it travels and is accessed. Each of these attributes can make online speech powerful. And each complicates the task of regulation.

Disinhibition in online speech is a much studied but not well-understood phenomenon. It accounts for greater responsiveness and "sharing" when we interact with social media, and also for greater informality, incivility and invective. While it is common to attribute disinhibition to anonymity, disinhibition is characteristic of attributed online speech as well, and various studies cite many factors that contribute to this quality, including the rapidity and impersonality of a medium lacking nonverbal cues and interaction. In fact, being identified (so peers can see you as the nastiest troll on the site) may worsen behavior. This complexity suggests that real-name policies are not necessarily a sure-fire way to better behavior. They are, however, a favorite requirement of authoritarian regimes that would like to identify dissenters so they can be silenced.

The persistence of online information advances all types of research and news gathering, long after first reports. Real-time fact-checking in political contests, for example, can add immeasurably to informed decision-making in elections. But malicious or false speech also persists, and even when the subject succeeds in having it retracted in one jurisdiction, it may be mirrored or available from another.

The European Court of Justice considered this problem in the 2014 *Costeja* judgment, and pronounced that search engines like Google had an obligation to delink to data that is "inaccurate, inadequate, irrelevant or excessive"—a standard that potentially allows for much more sweeping restrictions on public access to information than allowed under international human right standards or some national constitutions. A European view of what is "irrelevant" or "excessive" information, for example, might strike a US court as a violation of the First Amendment guarantees of freedom of speech; the information might well still be accessible in the US even if delinked from search results in Europe.

The persistence of information on the web and its global accessibility has prompted courts in Canada and France to issue orders to Google that would require the web index to delist content the world over, and not just within the court's home jurisdiction. But if Canada and France prevail, global injunctions against content or links to content can be expected to become *de rigeur*, including from countries that routinely punish dissent. Would more rights-respecting countries enforce such orders?

We may not even get to that question. Such injunctions would place the burden of challenge on the speaker, not on the party that wishes to suppress the speech. People who place controversial material on the internet may lack the means to challenge such orders in every country. The force of global injunctions is their chilling effect. They might reduce the amount of content some countries consider unlawful, but they might also purge the internet of much art, heterodoxy, criticism, and debate.

Finally, the trans-border accessibility and routing of online communications empowers those far from the social and commercial hubs where information concentrates, be they villagers, or rebels in the hinterlands. Governments have sought to control data by requiring it be kept within their borders to facilitate surveillance, or by using firewalls to keep undesirable content out. This may seem appealing in the context of limiting the influence of terrorists, intellectual property thieves, or those who shame and expose their victims. It is less attractive when considered from the point of view of dissenting authors and activists who throw their thoughts over the firewall, hoping they will live and be accessible elsewhere on the net.

The combination of these attributes—prolific, often unguarded sharing, accessible through time and across borders—makes possible not only scientific, artistic or even criminal collaborations as never before, but also frightening potential for comprehensive social profiling and persecution. Data mining, aggregation, and retention are increasingly in the human rights spotlight as new and potent dangers to freedom. This led prominent internet archivist Brewster Kahle to remark, "Edward Snowden showed we've inadvertently built the world's largest surveillance network with the web."

The new problems raised by the distinctive features of online speech seem to require doubling down on privacy and freedom of speech, rather than giving up on them. The internet is not some unusual and threatening medium, but increasingly the ordinary means of transmitting every type of speech and information in our world. It is not a state of exception, and the baseline rule in human rights law is that full observance of rights such as free expression and privacy is the norm; it is limitations that must be exceptional.

When Technology Changes, Human Rights Standards Still Fit

Back in 1948, the drafters of the Universal Declaration of Human Rights had the foresight to insulate one of the most fundamental rights from obsolescence. Article 19 of this foundational UN instrument provides:

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* (emphasis added).

Since then, the principle that all rights that apply offline apply online as well has been reiterated by the Human Rights Council and the General Assembly. While new media pose new challenges, there is little support for the view that somehow the advent of the internet has made human rights less important, or subject to entirely different standards.

The basic principles for evaluating whether restrictions on free expression, access to information, association, and privacy are consistent with international human rights law are well-established and reflected in many regional and domestic legal systems. The Human Rights Committee, the UN expert body that interprets the ICCPR, in 2004 summarized the basic framework this way:

States must demonstrate their necessity and only take such measures as are proportionate to the pursuance of legitimate aims in order to ensure continuous and effective protection of Covenant rights. In no case may the restrictions be applied or invoked in a manner that would impair the essence of a Covenant right.

Consider the test of "necessary" to a "legitimate aim," that is, an aim specified in the ICCPR, such as national security, public order, or the rights of others. The state bears the burden of showing "a direct and immediate connection" between the right to be restricted and the threat. It would not be enough, for example, for personal information to be collected simply because it might be, at some undefined point in the future, useful in advancing a variety of national interests.

In the context of the most common justification for electronic surveillance, the special rapporteur stated that "States often treat national security and public order as a label to legitimate any restriction." Such interests are understood in human rights law to represent the public's interest, rather than the interest of a particular government or elite. So "national security" should be seen as public interests in maintaining national independence or territorial integrity, not some individual’s or group's concern about staying in power or maintaining an edge over competitors. Invidious discrimination is never in the public's interest, and cannot be the basis of a valid limitation on rights, so surveillance measures that are directed at religious, ethnic, or national groups cannot be justified as "necessary" for "public security."

Dragnet collection and prolonged retention of masses of irrelevant personal data would normally be difficult to justify as "necessary" in the sense of directly connected to a specific threat to national security or public order. But, as noted above, international human rights law requires that laws restricting speech be “proportionate” as well as necessary, and it is even harder to show that sweeping surveillance measures meet that test.

To be proportionate, a limitation on rights must be the least restrictive means to protect the public interest that motivates the restriction. It is hard to imagine how regularly invading everyone's privacy, and monitoring everyone's communications could be proportionate to a specific threat, even the threat that a particular terrorist movement poses. Indeed, such practices would seem to "impair the essence of the right."

The special attributes of the internet can make old problems—whether terrorism, threatening speech, discrimination against minorities, or crime prevention—seem more daunting and in need of new solutions. But our obligation—if we think rights have meaning—is to still subject every solution that limits rights to rigorous consideration of necessity and proportionality.

Applying the Standards to Today’s Challenges

Law enforcement figures have argued that to identify terrorists and prevent attacks, a large "haystack" of data must be assembled to search. This presumes that more data will yield more relevant data to be mined, producing more "needles" constituting true threats. This may work for problems where instances are abundant, and the risk factors are relatively easy to identify.

But terrorists and terror plots are relatively rare and quite varied in profile, motivation, and details. The danger is that false leads can overwhelm the system and divert resources from more productive actions, such as developing reliable networks of informants or mining a suspect’s past criminal history for clues.

As security expert Bruce Schneier said in his recent book, *Data and Goliath*, "there is no scientific rationale for believing that adding irrelevant data about innocent people makes it easier to find a terrorist attack, and lots of evidence that it does not." Even the NSA has urged its personnel to "store less of the wrong data." The more irrelevant data is added to the "haystack," the harder it is to justify the collection program as proportionate. But when mass collection also leads to mass data retention, further questions arise. One is whether data collected for one purpose (say, foreign intelligence) can be later used for another (say, enforcement of drug laws).

Unless each use depends on an independent evaluation of necessity and proportionality, repurposing data cannot be sure to comply with human rights law. And simply retaining data for some hypothetical future use is difficult to justify as "necessary." As Norway's Supreme Court recently held in a case considering seizure of documentary maker's footage, the possibility that the material may contain "valuable clues" to the prevention of terrorism recruitment was not enough to make its disclosure "necessary."

Another problem is the use of biased data for predictive purposes. Corporations have long been aggregating and analyzing data on consumers to predict what advertisements, news, or job listings most suit their profile. Data protection law can offer some protection against this profiling by making what corporations do with your data more transparent, and enabling you to correct data or refuse to provide it.

But when governments use data analysis to predict where police should be directed, or whether a defendant with a particular profile is likely to recidivate, there is often little transparency as to what data was used to train the algorithm—and biased data produces biased results. Law enforcement practices all too often reflect bias, as Human Rights Watch has shown with relation to police profiling of immigrants and Muslims and racial disparities in arrest and incarceration in the US, abusive identity checks of Muslims in France, or police discrimination against transgender people in Sri Lanka. Algorithms that are trained on biased data can reinforce and even exaggerate biased profiles and policies, in a horrible self-confirming loop.

Surveillance, even when justified, involves limiting rights, but bias can turn this into discrimination or even persecution. When a person's faith, ethnicity, sexual orientation, or race are taken as indicators of potential criminality—by police or by the algorithm—their rights are violated. Programs for "countering violent extremism" can fall into this trap when they focus as much on the expression of "extremist" beliefs or opinions as on any indicator of actual violence.

The UK's "Prevent" strategy, for example, defines its objective as countering "ideology"—that is to say, ideas—and defines "extremism" as "vocal or active opposition to fundamental British values." Schools, and thus teachers, are obliged to monitor children's online activity for signs of radicalization, and intervene with those who are "vulnerable." The program has drawn widespread criticism from teachers for stifling free expression in the classroom, and from many as stigmatizing and alienating precisely the segments of the community that law enforcement most needs help from in identifying threats.

Applying the principle of proportionality, we see the more a program limits rights for the many, the less likely it is to be the least intrusive means of protecting security. Indeed, pervasive rights intrusions themselves can worsen national security or public order by eroding trust in government and protection of minorities. A case in point are laws that undermine anonymity, like Russia's, or that require companies to somehow decode encryption, like China's. No doubt some criminals use these strategies to evade detection, but ordinary people use them as well, to evade persecution, secure transactions, or simply ensure privacy in normal communications and pursuits.

Neither anonymity nor encryption are absolute rights; a court may order that a criminal suspect be identified, or require a person to decrypt their communications as part of an investigation. But disproportion is likely when governments claim it is necessary to compromise the rights and security of millions of users to catch specific bad guys by forcing companies to provide "back doors" into secure technology.

When the US Department of Justice, eager to get into the San Bernadino shooter's iPhone, tried to force Apple to re-engineer its security features, much more than that specific phone's security was at stake. This "fix" could be leaked or hacked by criminals who would seek to open the same models. Nor was there any guarantee the US government, or other governments, might not demand or use it repeatedly jeopardizing the security of all users of that model.

Governments can't evade their human rights obligations by pushing the burden onto companies to suppress uncivil speech, de-index information or retain unnecessary data. The effect on rights can be as disproportionate as if government had limited rights itself. Private companies, however, have considerable discretion to set the rules for their services, and these terms can be much harder for users to challenge than government-made laws.

Before urging internet service providers to monitor or bank all incoming traffic or provide back doors in security features, governments should consider the human rights impact. Even when civic groups urge corporations to enforce values like civility, we should consider whether these corporate rules will be transparent or opaque, capable of challenge, or driven by the sort of rights-blind algorithm that cannot tell the difference between pornography and photojournalism.

Realigning State Practice with International Standards

Limiting rights only where necessary and proportionate does not make regulation impossible. Some limits are essential, because protecting people from terrorism, incitement to violence, or revenge pornography is also a human rights obligation. We know that these principles are being taken seriously when there is transparency in law and state practice, independent oversight of executive powers, and avenues of appeal and redress.

Restrictions should apply to the fewest people and the fewest rights possible for the shortest period. And we have to consider whether some issues need state action, or are better addressed by communities, or new technology, or by enabling and promoting counter-speech. Finding the least intrusive means takes some imagination, and some collaboration between those who govern and those whose rights are at stake.

The present split between what states say and what they do cannot be sustained indefinitely. Either rights will take a beating in the digital age, or state practice must reconnect to rights protection.

Human rights and security are two faces of a single coin. When rights are consistently violated, societies become insecure, as anyone watching the destruction of Syria can tell.

Societies that deprive their inhabitants of online privacy and means of digital security are deeply vulnerable—to crime, to demagogues, to corruption, to intimidation, and to stagnation. Hurtling into a digital future, it seems prudent to carry our rights along, rather than abandon them by the roadside with our typewriters.