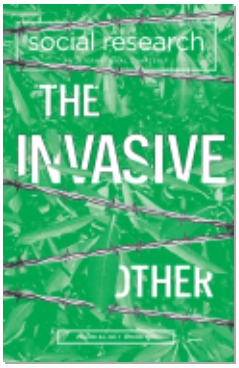
The Control of "Invasive" Ideas in a Digital Age

Agnes Callamard



Social Research: An International Quarterly, Volume 84, Number 1, Spring 2017, pp. 119-145 (Article)

Published by Johns Hopkins University Press

Agnes Callamard

The Control of "Invasive" Ideas in a Digital Age

INTRODUCTION

With the end of World War Two, it seemed that much of the world emerged resolute to turn away from the horrors of genocide and massacre, as well as from authoritarianism, central control, and heavy censorship of any and all ideas deemed invasive and challenging of authority. The United Nations was established, international human-rights standards were introduced, the free market and free trade developed, and liberal democracies flourished—at least in some parts of the world. These developments also cleared the way for freedom of expression to become an international human-rights norm and, as such, to gain state protection.

Some 60 years later, the advent of the Internet constituted a significant, even radical and historical turning point in the realization of freedom of expression. The Internet not only proclaimed and enabled the global exchange of ideas across borders; it also announced the advent of a new world—a world without sovereignty, a world of no government, no central control. The vision of this first digital generation was to unleash a new social contract: with a truly global technology, a new (online) world was to emerge, and its rules and governance would arise organically (Barlow 1996). In that new world, ideas were to flow unhindered, largely uncontrolled except by the working of the technology. These were Internet "genesis" claims, hyperbolic but not entirely beyond the realm of reality.

Not surprisingly, in this new world, conceptions of freedom loomed far larger than notions of control or censorship. Regulation, censorship, and control of ideas could only be conceived as the collateral "damage" of technological developments, of glitches in need of corrections, reached through a collective and transparent process. The early-days Internet was off limits to legislation and control by political authorities and institutions, the traditional instruments of censorship.

Such a state of affairs (as idealized as it may have been by Internet founders) shifted progressively and then considerably over the past decade, with Internet management and governance the object of a range of competing and acrimonious claims. The governance of the Internet, of which regulation and censorship are key elements, has become a central subject of inquiry and concern, at the heart of international disputes, amongst states and between state and nonstate actors.

If the initial vision of a free flow of information across frontiers is no longer the order of the day, what kind of freedom and what kinds of control and censorship have emerged in the online world of the 2010s? Has the revolutionary technology unleashed and allowed control over ideas, as unprecedented as the global exchange of ideas it has also permitted?

THE INTERNATIONAL FREE SPEECH REGIME

Ideas have been censored throughout history—from the banning of Bibles produced in the vernacular German language to the burning of books in Nazi Germany and the purging of artists and writers in the Soviet Union—because they were perceived and defined by those in power as threatening the cohesion of a community (geographically based or not), the mores and/or the orthodoxy of a dogma upon which the community, the country, the church, or the state is founded. In the views of the state or the church, such ideas were akin to an invasion of organized marauders intent on challenging or destroying the status quo, the order of things, the way society thought of itself, the systems of power allocation and distribution.

From Socrates' death by poison for impiety and corrupting the minds of the youth of Athens, to the censors in Rome responsible for both public accounting and oversight of mores in society, and to the early days of the Inquisition—all of these testify to the existence of organized control over ideas as a method of governance and of the preservation of power structures. The advent of Gutenberg's printing press and its capacity for mass production of information—and thus the development of a new and expanding literate class—heightened the necessity of censorship from the standpoint of those in power.

Censorship by church and state, in turn, produced resistance, resulting in the adoption of the 1689 English Bill of Rights, the United States Declaration of Independence in 1776, and the 1789 French Declaration of the Rights of Man. Through resisting censorship, philosophers developed the notions of autonomy, truth, and knowledge, all of which gave birth to the notion of a citizen's inalienable rights, including the right to freedom of expression. Rightsholders, however, were a defined category limited to men,[1] but only white and non-Jewish men. The Enlightenment resistance to censorship had been only partially unleashed and understood. Many ideas, particularly those related to the status of women, Jews, and blacks, remained "invasive," including in the minds of many who had fought (and even died) for the right to speak and access ideas.

The developments of the latter half of the 1940s, in reaction to the atrocities of World War Two, with its 40 million civilian deaths by genocide, massacre, famine, and censorship,[2] largely gave credence to a conception of censorship as the expression of arbitrary domination, with freedom of expression becoming a firmly established idea (although not necessarily a practice) both domestically and nationally as a fundamental right, inherent to all human beings, and an essential feature of liberal democracy.

As early as 1946, at its very first session, the United Nations General Assembly adopted Resolution 59(I), which states: "Freedom of information is a fundamental human right and … the touchstone of all the freedoms to which the United Nations is consecrated" (UN

1948a). Two years later, the Universal Declaration of Human Rights (UDHR) called for "the advent of a world in which human beings shall enjoy freedom of speech and belief and freedom from fear and want has been proclaimed as the highest aspiration of the common people" (UN 1948b). And in Article 19, the UDHR proclaims, "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."

This is the strongest expression ever of a universal commitment to freedom of expression, one that has never been repeated since. Indeed, in subsequent international developments, limits were attached to the exercise of the right.

At the time of the adoption of the UDHR, member states and UN officials were expecting that within one year they would have drafted and adopted a convention on human rights—meaning an enforceable and binding treaty. In fact, more than 18 years passed before the convention was adopted on December 16, 1966, a delay reflecting the Cold War polarization and the significant differences between the Western bloc's eagerness to codify civil and political rights, and the Soviet/Communist bloc's eagerness to protect economic rights; both blocs resisted what they considered to be invasive and unwelcome ideas. Nowhere was this opposition more sharply expressed than in the field of freedom of expression and the press, a state of affairs described at the time by the Canadian legal scholar John Humphrey (1984, 36), one of the drafters of the Universal Declaration of Human Rights, as "the deep incompatibilities between the communist and liberal approaches to the functions of the Press." By the time the International Covenant on Civil and Political Rights was finally adopted, the right to freedom of expression had evolved from its initial absolutist interpretation to a far more restrictive reading.

In Europe, governments had taken resolute steps toward European integration, to ensure that the horrors of World War Two would never be repeated, including by protecting against the fascist

ideologies that had made such horrors possible. The development of a Western European bloc also became a central instrument to protect against and counter the spread of communism. This integration was consecrated through the establishment of the Council of Europe (1953) and the adoption in 1950 of the European Convention on Human Rights. European states too were eager to protect and enshrine freedom of expression. But they were committed to doing so with a number of caveats attached. Paragraph 1 of Article 10 of the European Convention on Human Rights very much follows the wording of the UDHR stated above:

> 1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers.

Article 10 does not end there. It goes on to state, in paragraph 2:

> 2. The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary. (emphasis added)

Paragraph 2 of Article 10 of the European Convention has very much become a global norm, reflected more or less word for word in Article 19 of the International Covenant of Civil and Political Rights (ICCPR) and the regional conventions of the American and African continents.

The drafters of the successors to the 1948 UDHR introduced two important caveats to the initial absolutist understanding of freedom of expression under the UDHR: the notion of "duties and responsibilities," and a list of several grounds that could justify limiting freedom of expression.

Censorship versus Regulation

The parties involved in drafting these conventions did not seek to identify which ideas would be considered "invasive," with the notable exceptions of war propaganda (Article 20[1] of the ICCPR), incitement to genocide (Genocide Convention), other forms of incitement (Article 20[2] of the ICCPR), and racist hate speech (Article 4 of the International Convention against Racism). These are the only expressions or ideas against which sufficient international consensus could be mustered to allow for their inclusion in treaties, and even these ideas have been the object of a number of reservations on the part of some member states that did not fully agree with their prohibitions or criminalization.

All other forms of speech, international human rights declare, may be uttered but also legitimately restricted, provided the restriction meets these three criteria: it is prescribed by law; it serves one of the prescribed purposes listed in the international or regional conventions, including national security, reputation, rights of others, etc.; and it is *necessary* to achieve the prescribed purpose.

International human rights conventions do not refer or use such terms as "censorship" or "control." Speech may be or should be restricted. It may or should be prohibited or even criminalized. But it is not censored. The international human rights system post-World War Two has established the parameters for the legitimate censorship of information and ideas, although this is not how it is labeled. Instead, member states, the United Nations, lawyers, judges, the media, and press freedom organizations speak of speech or content or media "regulation" as a legitimate form of proscribing communication.

"Censorship," on the other hand, is what takes place outside the legal boundaries set up by the international and regional conventions:

> Boiled down to its essential elements, the liberal conception of censorship sees it as *external, coercive and repressive* ... Censorship is external in that it represents authorities' intervention in the sphere of consensual actions of individuals … It represents an act of arbitrary power. (Bunn 2015, 29–30, my emphasis)

Everything else, as long as it takes place within the carefully worded parameters of international law, amounts to *regulation*, legitimated by international law.

CONTROLLING INVASIVE IDEAS IN A DIGITAL ERA: GLOBALIZED CENSORSHIP

There is no doubt that the 50 decades following the adoption of the international human rights regime have been characterized by marked improvement in the human rights situation of people around the world, for both civil and political rights, but also for economic rights. A legalized management of freedom of expression, away from the arbitrary decision of a nonelected leader, has progressively been endorsed by an increasing number of states, from Latin America in the 1970s and 1980s, to Eastern Europe in the 1980s, to Africa. This is largely reflected in the increasingly complex and sophisticated regulation, policymaking, and jurisprudence on and around the media and freedom of expression, and the numerous public debates on the legitimacy of such and such expression.

On the other hand, the international and regional conventions, which have accompanied and given significance to the post-war international system of content regulation, have not been implemented systematically or consistently. This was true of the years following the establishment of the human rights system,[3] and it is true now.

Indeed, empirical evidence suggests that the gap between the conventions and practice has been increasing, particularly since the early years of the twenty-first century, signaling a return in force of censorship (arbitrary, external, and repressive), away from regulation.

There is an extensive body of work and publications by human rights and press freedom organizations, including yearly indices and reports, documenting a decade of global setbacks as far as freedom of expression is concerned. In 2015, Freedom House documented the tenth consecutive year of decline in global freedom (Freedom House 2015a), and Amnesty International has spoken of a "global assault on freedoms" (Amnesty International 2015). The misguided reaction of many governments to national security threats has been the crushing of civil society, privacy, and free speech, and even outright attempts to smear and denigrate human rights, packaging them in opposition to national security, law and order, and national values.

These developments are reflected in the imprisonment of too large a number of journalists (CPJ 2015), human rights defenders (Front Line Defenders 2016), or others who speak out, and even their killing at the hands of the state or—increasingly—nonstate actors, including "terrorist" groups and the violent arms of powerful corporations and business interests (Front Line Defenders 2016).

Such a development is arguably triggered by a range of factors external to the nature of the communication and information environment, such as the reordering of the international system, a lingering economic and financial crisis in many regions of the world, and rising inequality, not to mention 9/11. However, "internal" factors, meaning the new technology of information itself, also account for the return in force of censorship as both a global and globalized phenomenon.

The Internet, social media, and search engines have radically transformed expression, information, and communication. According to the latest information regarding the Internet, there are currently some 3.5 billion people online, or about 40 percent of the world population, as against 1 percent in 1995 (see http://www.Internetlivestats.

com/Internet-users). This figure means that there are potentially 3.5 billion people around the world who are, at the very least, accessing information produced by others *anywhere in the world*. Furthermore, these 3.5 billion people are not just consumers of ideas or news, but also potentially their *producers:* of online videos, movies, radio programs, opinions, news, art, and so on.

The incredible revolutionary power of this new information technology stems from the number of people involved, simultaneously, as both consumers and producers; the billion ideas and bits of information that may be produced by a click; the borderless nature; and the speed at which information travels.

The transborder nature of almost all information flows, along with the central role played by nonstate actors in its creation and circulation—including corporations, engineers, and users—have raised large problems for a regulatory system based on national sovereignty: how can the state effectively control information and ideas that it has deemed "invasive"?

Some methods of control in the digital era are similar to those practiced in the previous decades, involving silencing speakers, often enough by relying on vague and overbroad laws coupled with arbitrary decisions. They do differ, though, first and foremost in the globalization and normalization of censorship, achieved in this second decade of the twenty-first century, through the clear and quasi-global consolidation of national security as an all-encompassing *global* framework—in law, mind, and spirit—and subjected to little opposition and limited debate.

The Tipping Point to Globalized Censorship? Countering Terrorism and Surveillance

In 2013, Edward Snowden's revelation of massive Internet surveillance by the US and other governments pointed to the state reasserting its full control over a technology and an industry that many thought had grown and extended beyond its reach. But there had been a multitude of early warning signs before then.

The last decade or so has witnessed the multiplication of regressive laws and policies: laws concerning terrorism, the Internet, protests, associations, and so on. It is nothing short of a viral spread of repressive laws targeting nongovernmental organizations (NGOs) and human rights defenders; social media activists and social media; independent press; and religious, ethnic, or indigenous groups—and it has been recorded by NGOs, academics, and some governments alike (Front Line Defenders 2016).

Such laws are far more about enshrining censorship (repressive and coercive) than they are about regulation of content deemed illegitimate under international human-rights law. They include provisions requesting the registration of online sites, bloggers, and citizen journalists; the filtering and blocking of access to content online, including entire websites, IP addresses, ports, network protocols, or certain types of uses; and Internet shutdowns—all of which go way beyond the permissible restrictions on free speech under the post-World War Two human-rights system.

The legal arsenal is particularly marked in the area of "national security," with terrorism and counterterrorism emerging in the 2010s as a tipping point to greater legalized censorship.

The development of the Internet and the multiplication of its capabilities over the past decade have taken place alongside the internationalization, expansion, and further deterioration of the conflicts in the Middle East, West Africa, North Africa, and most recently Ukraine, as well as the geographical expansion of "terrorism" and an increase in terrorism-related deaths (Institute for Economics and Peace 2015). A pervasive position held by states is that the Internet, and particularly the social media websites Twitter and Facebook and the messaging service WhatsApp, have acted as formidable allies to "terrorist" groups such as ISIS, and constitute a major platform and vehicle for the so-called process of "radicalization." Accordingly, a major focus of the policies designed to counter terrorism has been the online world.

A Human Rights Watch 2012 report identified more than 140 countries as having adopted counterterrorism laws following 9/11, and found that 130 of those laws contained one or more provisions that opened the door to abuse (Human Rights Watch 2012). Such laws come in addition to the laws on cybersecurity, laws on on-line expression, and sedition laws, all of which include or focus on regulating the ideology of "terrorism."

On the surface, the response is in keeping with the requirement of "legality" found in international conventions with regard to the regulation of speech. This is on the surface only. What has happened is a global legalized attack on the idea and practice of freedom of expression, in the name of national security, through the adoption of new legal offenses, the use of new sociological categories, and the stretching of established legal norms, as well as a skewed balancing of interests to the detriment of freedom of expression and civil liberties (Doyle 2010; Stone 2004).

Spurious Legal and Sociological Categories of "Deviance"

The focus on protection from certain ideas (largely religious) has been strengthened by the emergence of new policy and sociological categories: the "radical" and "extremist."[4] The result is an amalgam and conflation of the concepts of terrorism, extremism, and fundamentalism, often enough used interchangeably, even though they ought to carry very different legal, policy, and social understandings and implications. According to the UN Special Rapporteur on the protection and promotion of human rights while countering terrorism (HRC 2016): "Some States have misused these poorly defined concepts to suppress political opposition or ideological dissent from mainstream values," and "legislation against extremism has in some instances been used against journalists, religious groups or critics of state policy and this is not acceptable." Altogether, they have resulted in excessive interferences with freedom of association, expression, and the media. Accusations of "terrorism" are levelled against perfectly legitimate (under international human-rights law) actions by human and

women's rights defenders, political opponents, journalists, and religious leaders.[5]

Judicial Complicity

Such an evolution has required the complicity at worst, or lack of critical judicial engagement at best, on the part of legal institutions, which have tended to uphold and give legitimacy to badly drafted and rushed legislation, or have focused on the ideological and religious roots of "terrorism" rather than on a possible nexus between expression/ideas and the use of violence (Callamard 2015; UN 2016).

Judges in particular had the opportunity to address the vagueness and overbroad nature of many antiterrorism laws recently adopted. They could have done so by providing clear legal directions and tests to weaken the arbitrary or overbroad nature of the laws or by ruling that the legal uncertainty created by the vagueness of a law had to benefit the various defendants. This, however, they have done only on a few occasions, such as, for instance, the Norwegian Supreme Court in 2015 in the case of *Rolfsen v. Norwegian Prosecution Authority* (https://globalfreedomofexpression.columbia.edu/cases/rolfsen-association-norwegian-editors-v-norwegian-prosecution-authority/). As my analyses of a large number of decisions have led me to conclude, courts and judges have taken shortcuts, "instrumentalising not only speech to perceived higher needs, but judicial reasoning and practices as well" (Callamard 2015). This may be in keeping with historical responses to "invasive" ideas, particularly when these are said to be affecting national security. In his review of Geoffrey Stone's (2004) work on free speech in the United States during wartime, from 1798 to the war on terrorism, Lee Bollinger (2005) points to an important finding of Stone's detailed historical review: judges rigidly invoke their official obligation to enforce the law and actually overlook or ignore reasonable interpretations of that law that would moderate its harmful impact on civil liberties in general, and free speech in particular.

Digital Surveillance

The consolidation of national security as an ever-present global framework has been further facilitated by digital surveillance, a seemingly ubiquitous phenomena involving

> the state collecting and potentially analyzing everyone's every click online; cell signal catchers transmitting not only our calls and all associated data to government agencies; officials combing through our social media postings for whatever they consider "extremism," even government-deployed hackers taking over our computers in an effort to track us digitally. (Pokempner 2016)

The massive (meaning indiscriminate, disproportionate) nature of state digital surveillance makes it an important tool of censorship through the chilling effect it creates by precluding or preventing the exploration of dissent, controversial ideas, and reaching out to certain groups or people.

In the security-obsessed world of the twenty-first century, the indiscriminate nature of digital surveillance is justified by insisting on the necessity to control certain selected groups of people by decrypting, if not "predicting," how their profiles differ from the "average." The French sociologist Didier Bigo (2006; 2008) has coined the term "ban-opticon" in reference to both the globalization of the security field and the exclusion of certain people (potential terrorists, refugees, migrants), not on the basis of who they are, but largely on the basis of what they may become.

In a later article, written in the aftermath of Snowden's revelations, Bigo and his coauthors (Bauman et al. 2015) move away from the focus on surveillance-as-exclusion to surveillance-as-massive: ubiquitous, permanent, familiar, banal, and routine. In the digital era, surveillance is certainly key to the state but it is also at the heart of the spectacle society, and the information economy, which captures, analyzes, and indexes the personal data of billions of us-

ers (Lyon 2003; Gandy 2005). State surveillance, and the other side of the coin, censorship, are thus made possible by the complicity of the surveillance targets (the vast majority of online users) and a technology that strives and multiplies on the collection, use, and analysis of personal data.

PRIVATE, CLOSE, AND PERSONAL

Censorship in the digital era is historically notable for the globalization of the phenomena. It also exhibits a few more characteristics: it is increasingly privatized, personal, and technologically grounded.

Censorship by Proxy

A major feature of the current response to "invasive" ideas is the co-option of a range of nonstate actors, particularly corporations, in the monitoring of "invasive" ideas, or what others have termed the "privatization" of censorship. This process has been particularly well reported in the context of counterterrorism, where, on a regular basis, social media platforms are called upon by the state and members of the public to better police the Internet for "extremist" content, with a view to deleting the offensive content, or assisting the state in counter-messaging (see, for example, http://www.cnn.com/2016/02/24/politics/justice-department-apple-fbi-isis-san-bernardino).

In effect, governments are shifting the burden of censorship onto private social media companies and their users, not only by forcing them to delete or block content on demand, but most crucially by insisting they establish their own monitoring or controlling system to track and delete "terrorist content" (Freedom on the Net 2015; CPJ 2015).

To do so, these companies rely on a range of technological means (algorithms) to track down "terrorist" ideas for the purpose of blocking, deleting, and possibly reporting to state authorities those ideas that have been deemed unacceptable. They have also a small army of human monitors, riveted to their screens all day, searching for "terrorist," "violent," or "offensive" content. They even rely on

their own users to complain about or flag not only "terrorist" but also "offensive" content.

This kind of content regulation (or is it censorship?) may respond to national laws and specific state requests, particularly with regard to "extremist" or "terrorist" content, copyright infringement, or obscenity. It underscores delegating responsibility for content regulation and censorship, away from the state or state institutions and to private actors. International law's insistence on the "specific duties and responsibilities" of nonstate actors in the legitimate regulation of speech may have allowed or indeed demanded the expanding role of the online corporations.

There are, however, two other dimensions to the control of invasive ideas in the digital era: the privatization and personalization of the control.

The Privatization of Censorship

The role played by social media corporations in imposing their own understanding of what does and doesn't constitute legitimate content, through their terms of service, has been the object of complaints and debates.

This kind of content regulation raises two intertwined yet distinct problems: one concerns the nature of the content that is being censored; the second the process through which such content is banned, blocked, or deleted.

Arguably, social media companies have tended to err on the side of a more absolutist and libertarian approach to free speech, tolerating a wide range of ideas and expressions, a situation that has prompted all states (with possibly the exception of the United States) to demand more gatekeepers and control. Still, an essential question of principle remains. Private companies are deciding, without checks and balances, and outside the law, what is and what is not acceptable and legitimate speech and ideas circulating on their platforms.

Corporations are regularly intervening to block content they deem obscene, for instance—a determination process and a catego-

rization of speech/content that many around the world are contesting. A case in point is breastfeeding, which is routinely censored by Facebook, while images and written descriptions of rape and violence against women are not. In September 2016, Facebook deleted from the Facebook pages of many accounts, including that of Norway's prime minister, a 1972 photograph by Pulitzer Prize-winner Nick Ut, showing a naked nine-year-old girl, Phan Thị Kim Phúc, fleeing a Napalm attack. The photo was deleted on the grounds that it violated Facebook's guidelines on obscenity. The decision sparked backlash across print and social media, and throughout the political spectrum as well. The incident served as a useful reminder of Facebook's problematic cultural constructs and its process for determining what may or may not violate its rules.

From a content standpoint, at issue are the explicit and implicit American cultural, legal, and political references adopted by these Internet corporations. As a general rule, the First Amendment's strong protection of freedom of expression does not apply to spaces that are privately owned, including private school campuses, shopping malls, and corporations (*Hudgens v. NRLB* 1976: https://www.law.cornell.edu/supremecourt/text/424/507). American Internet companies are thus at liberty to impose content regulation that would not be tolerated if the censor were the state.

The terms of service of American Internet platforms have also tended to reflect a First Amendment conception of free speech, with content regulation focusing on what the First Amendment doctrine has qualified as "low" value speech—in the first place obscenity, one of the few ideas that may be legitimately censored under the First Amendment. However, such an approach is not necessarily supported by international human-rights law.

> [T]his censorship takes place outside the scope of internationally recognised standards governing the permissible limitations on freedom of expression … The problem … is further compounded by the lack of transparency in the way these restrictions are implemented; the lack of clear

> guidelines that users can refer to; and the absence of appropriate mechanisms for users to appeal against decisions by ISPs to censor user-generated content. This effectively means that online content is increasingly being regulated and censored via private contracts that offer limited transparency and accountability. (ARTICLE 19, 2015)

The *process* for content regulation also raises problematic questions. Who or what is to regulate, and who or what ends up being censored? A new technology of censorship has developed, mirroring the automation of economic, social, and military activities, raising a range of legal and ethical concerns over who controls what, and how far the automation of censorship goes. In the oft-cited September 2016 deletion of the girl-fleeing-napalm photo, Facebook appears to have relied on automated tools to monitor and delete the problematic content. In a subsequent apology letter, Facebook conceded, "These are difficult decisions and we don't always get it right … Even with clear standards, screening millions of posts on a case-by-case basis every week is challenging" (Dagenborg 2016).

While human involvement may remain a better option from a human rights and ethical standpoint, *which* humans is undoubtedly a crucial question. Drawing an analogy with the citizen informants of Communist East Germany during the second half of the twentieth century, Jillian York (2016) denounced the reliance on users for giving rise to "an online snitching culture, in which users are expected to monitor one another's actions and report problematic activity to the company."

Private corporations are not the only ones determining which ideas ought to be controlled. The digital users themselves may just as easily be their own censors.

Personalized Censorship

It has now become commonplace to argue that the Internet may function as an echo chamber (Sunstein 2007): online individuals find their ideas supported and echoed by other like-minded individuals, whom

they have picked, selected, "followed." Together they forge a transborder collective identity of a kind that may be properly unique in scope and breadth (O'Hara and Stevens 2015; Gerstenfeld, Grant, and Chiang 2003).

This process is reinforced or facilitated through algorithms analyzing personal data that social media companies have devised, inviting users to "like" or "follow" individuals with whom they appear to share similar interests or views, or to purchase products or read content tailored to their online profile.

The result is that just as the Internet promotes expanding one's world of ideas, it may just as easily promote reducing it: through a click, one may unlike, mute, block, "unfollow," while returning day in and day out to the same websites, news sources, and online chat rooms. The Internet, the revolution that can and should open one's mind to other realities, has the potential to just as easily close it.

Controlling the Technology and Undermining Its Founding Myths

The ubiquity of the Internet may make us forget that many governments are at war with the technology, and particularly with its global outreach in and out of "sovereign" spaces. The Chinese firewall, the national intranet of North Korea, Cuba, and now possibly Iran, are all examples of governments' suspicion of the technology and their determination to replace it with state-controlled and national systems—not only to fight "invasive" ideas from within and without national borders, but also to fight a "foreign" technology, controlled by the outside world.

The Internet is largely a US invention, and to this day it remains largely US technology, powered by US private actors supported or protected by the US government. The United States is still, to this day, the most powerful actor in cyberspace (Garton Ash 2016, 31).

The asymmetry between the United States and other governments, as far as the Internet is concerned, has become a central dynamic of its governance (Amoretti and Santaniello 2016), increasingly so as the Internet and information technology have founded the glob-

al information economy while transforming the actors and nature of security threats. This is an asymmetry resented not only by the United States' traditional enemies but many of its traditional allies as well. The fight is particularly well played out at judicial and normative levels in Europe. Such judicial drama may focus directly on the commercial behaviors of these companies,[6] but many others concentrate on the norms these corporations have embraced and sought to globalize. The ongoing dispute over the "right to be forgotten" (Callamard 2017) highlights the latter.

The right to be forgotten, or, more accurately, de-indexed, was unleashed in 2014 by a European Court of Justice decision, *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González* (2014), which applied a European directive on data protection (Directive 95/46/EC) to establish that search engines must erase search results and links to web pages providing private information that appear to be inadequate, irrelevant, no longer relevant, or excessive. As a result of the decision, anyone in Europe could request that search engines remove links to pages about themselves, even if the pages remain on the Internet, provided the information met certain criteria, e.g., inadequacy. In subsequent developments, the decision was referred to or mentioned by a number of courts in Europe and around the world. In 2015, the French regulator, as well as a Canadian court, insisted that to be meaningful the de-indexation must be applied to google.com, not just to the national Google entities, such as google.fr.

The right to be de-indexed has generated an extraordinary amount of debate and controversy, largely pitting the United States against Europe, and the global Internet and free speech community against those insisting on a right to privacy online and in the digital context. The decision and its implementation generate a number of issues, some of which go to the heart of the Internet vision, such as whether online information and data should ever be erased, whether there is a human right to have one's personal data erased in the name of privacy, the implications of the decision for freedom of informa-

tion and expression, and the possibilities or likelihood of abuse by those in power wishing to erase from public knowledge and public scrutiny disturbing truths. Global interpretation and implementation of the decision raise additional problems, particularly concerning the extraterritorial overreach on the part of states imposing erasure or de-indexation.

Users who have made recourse to the right to be forgotten do so to control an idea about themselves that *they* have experienced as invasive. This is not an idea that will disappear altogether from the online or even the offline world. But it is an idea that will be difficult to access when the online gatekeepers (search engines in general; Google in particular) are reined in.

From the standpoint of the founding working principles of the Internet in general, and search engines in particular, the right to be forgotten is a profoundly "invasive" idea, as the 1996 declaration on the independence of Cyberspace reminds us (Barlow 1996):

> Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather.
>
> Your increasingly obsolete information industries would perpetuate themselves by proposing laws, in America and elsewhere, that claim to own speech itself throughout the world. These laws would declare ideas to be another industrial product, no more noble than pig iron. In our world, whatever the human mind may create can be reproduced and distributed infinitely at no cost. The global conveyance of thought no longer requires your factories to accomplish.

In the digital world, patrolling and controlling "invasive" ideas, grounded upon what some or many may perceive as the inva-

sive working of the technology, is also done by imposing an invasive norm in return.

CONCLUSION

As early as 1997, Internet expert Tim Wu concluded a review of Internet regulation with these words:

> States, their governments, and their citizens ought never be taken for granted as players in cyberspace. It is easy, given the current state of the Internet, to assume that it is and will remain free of external regulation. However, it would be incorrect to adopt such an assumption. A quick empirical look suggests that it is possible to regulate the Internet, and that countries, corporations, organizations, and private individuals are already doing so. (1997, 665)

These actors are all involved in what may in fact increasingly amount to censorship, as opposed to the free speech regulatory regime enacted in the aftermath of World War Two.

A powerful indicator of the importance of the state is the multiplication of laws, policies, and regulations enacted to control the working of the online world, including by censoring the production and exchange of certain ideas and engaging in mass surveillance of digital users.

The return in force of the principles at the heart of the pre-digital world is well demonstrated by would-be norm entrepreneur China and its aggressive advocacy for an international recognition of "Internet Sovereignty" (Tiezzi 2014).

Europe's numerous regulatory and judicial fights with American Internet corporations are no less about sovereignty. Europe, though, in its disputes with US firms, is not challenging the principle of freedom of expression online (as China does) but is challenging a cultural interpretation and imposition of the meaning and extent of freedom of expression.

As far as the regulation and censorship of online invasive ideas are concerned, the notion of sovereignty has not disappeared; it has weakened, perhaps—though even that is increasingly doubtful—and been transformed, absolutely, but it has not disappeared. In the digital era, national sovereignty is not only about controlling the integrity of national territory (on and offline) but also about exercising it extraterritorially: through control over the technology institutional framework, surveillance, norms, and actors (US); through the courts and the imposition of competing ideas and online behavior and values (Europe); and through alternate technology, firewalls, hacking, and intergovernmental institutions (China).

But state-grounded censorship is only one determinant in the control of invasive ideas in the digital era. Indeed, that an increasingly external and repressive state censorship is being implemented alongside a privatized and personalized control over ideas, in the context of an often acrimonious, aggressive, bullish digital world, should give us some pause as to the nature of the global public sphere in this digital era.

Benjamin Franklin, upon the formation of the United States, asserted, "Whoever would overthrow the liberty of a nation must begin by subduing the freeness of speech." Speech on and off-line, in the digital era, is not subsumed in the way Franklin warned us against. But it is monitored, collected, and dissected in unprecedented ways; it may be blocked and thus prevented from reaching others, or deleted so that others can never access it. Online, it establishes digital transborder communities, whose self-selected members may just as quickly build digital walls to protect the integrity of their "territory." It is regulated by private companies whose primary accountability is to the market.

When the freeness of speech is subdued in such a fashion, how much liberty—on a personal, national, and global scale—is then imperiled?

NOTES

1. Olympes de Gouges famously combatted the exclusion of women from the French Revolution and its Declaration of the Rights of Men ("men" understood both literally and symbolically), and died for her combat. See her *Declaration for the Right of Women and of the Female Citizen* (1791). To this day, the language of human rights in French may be said to be exclusive rather than inclusive (see Callamard 1999).
2. On April 6, 1933, the German Students Association for Press and Propaganda urged the "cleansing" of literature and threw public festivals to celebrate the bonfires. On May 10, 1933, the largest of these book burnings took place, destroying some 25,000 copies of literature deemed "un-German." These included books written by Jewish, communist, and socialist authors, as well as select authors such as Ernest Hemingway, Jack London, Helen Keller, Sigmund Freud, and Upton Sinclair. Stalin, leader of the USSR, also in an effort to abolish Jewish culture, ordered the burning of Jewish books in his country in the 1930s and 1940s.
3. Within the Western world, in the 1960s and 1970s, a number of ideas were combatted, their speakers sometimes imprisoned or killed, including extrajudicially Ideas such as communism, equality between races and peoples, calls for self-determination, anticolonialism, were very much invasive ideas, invading both from within and outside. See for instance Jensen 2016.
4. The vast majority of countries around the world, whether touched directly or indirectly by acts of "terrorism" in the 2010s, have adopted some definitions or notions of radicalization, extremism, or violent extremism.
5. Such an outcome was well evidenced by the Turkish president, Recep Tayyip Erdogan, who announced in the aftermath of the third major suicide bomb attack to hit Ankara in 2016 that the definition of "terrorists" needed to be broadened to include "supporters" of terrorism, who could be considered equally guilty, such as authors and journalists (http://www.bbc.com/news/world-europe-35807987).

6. See, for instance, the recent European Commission landmark judgment ordering Apple to pay the Irish state up to 13 billion euros in taxes. Apple has paid a tax rate on European profits of between 0.005 percent and 1 percent (http://europa.eu/rapid/press-release_IP-16-2923_en.htm).

REFERENCES

Amnesty International. 2015. "Foreword." *Annual Report 2015/2015. The State of the World's Human Rights*, 14–17.

Amoretti, Francesco and Mauro Santaniello. 2016. "Between Reason of State and Reason of Market: The Developments of Internet Governance in Historical Perspective." Paper presented at the IPSA/AISP, 24th World Congress of Political Science, July 23–28, Poznan, Poland.

ARTICLE 19. 2013. *Internet Intermediary: Dilemma of Liability*. London: ARTICLE 19.

Barlow, John P. 1996. "A Declaration of the Independence of Cyberspace." http://editions-hache.com/essais/pdf/barlow1.pdf.

Bauman, Zygmunt, Didier Bigo, Paulo Esteves, Elspeth Guild, Vivienne Jabri, David Lyon, and R. B. J. Walker. 2015. "Repenser l'Impact de la Surveillance après l'Affaire Snowden: Sécurité Nationale, Droits de l'Homme, Démocratie, Subjectivité et Obeisance." *Cultures et Conflits* 98 (Summer): 133–66.

Bigo, Didier. 2006. "Security, Exception, Ban and Surveillance." In *Theorizing Surveillance: The Panopticon and Beyond.* 46–68. Cullompton, Devon, UK: Willan Publishing.

———. 2008. "Globalized (In)Security: The Field and the Ban-opticon." In *Terror, Insecurity and Liberty: Illiberal Practices of Liberal Regimes after 9/11*. Edited by Didier Bigo and Anastasia Tsoukala, 10–48. Abingdon: Routledge.

Bollinger, Lee. 2005. "The First Amendment's Original Sin (reviewing *Perilous Times: Free Speech in Wartime, from the Sedition Act of 1798 to the War on Terrorism* by Geoffrey R. Stone)." *University of Chicago Law Review* 72 (1): 417–28. http://chicagounbound.uchicago.edu/uclrev/vol72/iss1/20.

Bunn, Matthew. 2015. "Reimagining Repression: New Censorship Theory and After." *History and Theory* 54: 25–44.

Callamard, Agnes. 1999. "Le Sexisme à Fleur de Mots." *Maniere de Voir* 44: 10–12.

———. 2015. "Religion, Terrorism and Speech in a 'Post-*Charlie Hebdo*' World." *Religion and Human Rights* 10: 207–28.

———. 2017. "Are Courts Re-Inventing Internet Regulation?" *International Review of Law, Computers and Technology* (March) 1–17. http://dx.doi.org/10.1080/13600869.2017.1304603.

Committee to Protect Journalists. *2015 Prison Census*: https://www.cpj.org/imprisoned/2015.php. *Killed in 2015*: https://cpj.org/killed/2015.

Council of Europe. 1953. *European Convention on Human Rights*. http://www.echr.coe.int/Documents/Convention_ENG.pdf.

Dagenborg, Joachim. 2016. "Facebook Says Will Learn from Mistake over Vietnam Photo." *Reuters*, September 12.

De Gouges, Olympes. 1791. *The Declaration for the Rights of Women and the Female Citizen.*

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A31995L0046.

Doyle, Charles. 2010. *Terrorist Material Support: An Overview of 18 U.S.C. 2339A and 2339B*. Congressional Research Service, July 19.

Freedom House. 2015. *Freedom in the World 2015*. https://freedomhouse.org/report/freedom-world/freedom-world-2015#.V-hC7mV4zFI.

Front Line Defenders. 2016. *2016 Annual Report.* Dublin: Front Line, the International Foundation for the Protection of Human Rights Defenders.

Gandy, O. Jr. 2005. "Data Mining, Surveillance, and Discrimination in the Post-9/11 Environment" in *The New Politics of Surveillance and Visibility*, edited by Kevin Haggerty and Richard Ericson. University of Toronto Press.

Garton Ash, Timothy. 2016. *Free Speech: Ten Principles for a Connected World*. New Haven: Yale University Press.

Gerstenfeld, Phyllis B., Diana R. Grant, Chau-Pu Chiang. 2003. "Hate Online: A Content Analysis of Extremist Internet Sites." *Analyses of Social Issues and Public Policy* 3 (1): 29–44.

Human Rights Council. 2016. *Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism.* A/HRC/31/65.

Human Rights Watch. 2012. *In the Name of Security: Counterterrorism Laws Worldwide since September 11*. June 29. https://www.hrw.org/report/2012/06/29/name-security/counterterrorism-laws-worldwide-september-11.

Humphrey, John P. 1984. *Human Rights and the United Nations: A Great Adventure*. Dobbs Ferry: Transnational Publishers.

Institute for Economics and Peace. 2015. *Global Peace Index*. http://economicsandpeace.org/wp-content/uploads/2015/06/Global-Peace-Index-Report-2015_0.pdf.

Jensen, Steven. 2016. *The Making of International Human Rights.* Cambridge: Cambridge University Press.

Lyon, D., ed. 2003. *Surveillance and Social Sorting*. London: Routledge.

O'Hara, K. and D. Stevens. 2015. "Echo Chambers and Online Radicalism: Assessing the Internet's Complicity in Violent Extremism." *Policy and Internet* 7: 401–22. doi:10.1002/poi3.88.

Pokempner, Dinah. 2016. "Surveillance Within and Across Borders." Video for Columbia University's Global Freedom of Expression MOOC on "Freedom of Expression in the Age of Globalization." https://www.youtube.com/watch?v=TY5PMNcYdRA&feature=youtu.be

Stone, Geoffrey. 2004. *Perilous Time: Free Speech in Wartime.* London: Norton.

Sunstein, Cass. 2007. *Republic.com 2.0*. Princeton: Princeton University Press.

Tiezzi, Shannon. 2014. "China's 'Sovereign Internet'." *The Diplomat*, June 24. http://thediplomat.com/2014/06/chinas-sovereign-Internet.

United Nations General Assembly. 1948a. Resolution 59(I).

———. 1948b. *Universal Declaration of Human Rights*.

———. 2016. *Report of the Special Rapporteur on the Situation of Human Rights Defenders*. A/71/281.

Wu, Timothy S. 1997. "Cyberspace Sovereignty? The Internet and the International System." *Harvard Journal of Law and Technology* 10 (3): 647–66.

York, Jillian C. 2016. "Facebook and Twitter Are Getting Rich by Building a Culture of Snitching." *Quartz,* July 14. https://qz.com/731347/facebook-and-twitter-are-getting-rich-by-building-a-culture-of-snitching.