Government Control of Electronic Information:
The Finer Line Between Serving and Suppressing the Public Interest

Sorell E. Negro

> "What finally emerges from the 'clear and present danger' cases is a working principle that the substantive evil must be extremely serious and the degree of imminence extremely high before utterances can be punished. . . . It must be taken as a command of the broadest scope that explicit language, read in the context of a liberty-loving society, will allow."
>
> -Justice Hugo L. Black
> *Bridges v. California*, 314 U.S. 252, 263 (1940)

I. INTRODUCTION

Advances in technology have the potential to improve access to justice, increase transparency, and better meet people's legal needs. Examples of this include making documents filed in court electronically available and therefore more easily accessible to the public and allowing courts to process filings more quickly. The Internet also makes more transparent when local government commissions and boards are meeting and what is discussed by having agendas and minutes also electronically available. However, the advances in maintaining and sharing information electronically also come with risks of governments overstepping and crossing the sometimes fine line between acting in what is the purported public interest versus violating key rights—particularly privacy or free speech rights. Even worse, a government overstepping in this manner, or being perceived as overstepping, could result in the repression of speech and could stunt the growth of democracy. This article will discuss these important and emerging issues regarding the government's regulation and use of electronic data, and that seemingly finer line between serving the public interest and repressing fundamental democratic principles upon which free and open societies are built.

First, this article will discuss free speech rights in the United States with regard to electronic communications and recent developments in regulation of Internet and social media usage. It will then address the global challenge of balancing law enforcement needs with privacy protections and how various countries are addressing these issues with new or proposed legislation. Lastly, I will discuss examples of latent government abuses of the Internet and social media based on my experience in practicing land use law in a developing democracy. This paper will assess the effects that such repressive actions have on the ability of a democracy to function and what options are available to seek justice and pursue free speech under such circumstances.

II. GOVERNMENT REGULATION OF ELECTRONIC COMMUNICATIONS V. FREE SPEECH

A. Free (Electronic) Speech Rights in the United States

Governments around the world are struggling with balancing, on the one hand, government regulation and law enforcement needs and, on the other hand, free speech and privacy rights. Almost 20 years ago, in 1997, the U.S. Supreme Court held that the First Amendment's free speech protections apply to communications over the Internet. *Reno v. American Civil Liberties Union*, 521 U.S. 844, 870 (1997) ("'[T]he content on the Internet is as diverse as human thought.' . . . [O]ur cases provide no basis for qualifying the level of First Amendment scrutiny that should be applied to this medium.") (citation omitted). In 2016, particularly following the Court's 2015 decision in *Reed v. Gilbert*, First Amendment protections are seemingly as robust as ever. It remains to be seen what the full impact of this decision will look like on government regulation of electronic communications.

Reed v. Gilbert, 135 S. Ct. 2218 (2015), was called by The New York Times "the sleeper case" of the last Supreme Court term; it has been said to have "transformed" First Amendment law; and it has been predicted to have far reaching effects. Adam Liptak, *Court's Free-Speech*

Expansion Has Far-Reaching Consequences, N.Y. TIMES (Aug. 17, 2015), http://www.nytimes.com/2015/08/18/us/politics/courts-free-speech-expansion-has-far-reaching-consequences.html?_r=0. This case clarified, or some say, redefined, what types of government regulations of speech will be subject to the heightened standard of review by the courts known as "strict scrutiny," meaning they must be narrowly tailored to further a compelling government interest to pass muster. This is a very high standard to meet, and it is very rare that a regulation survives strict scrutiny.

Reed's definition of a content based regulation is indeed much broader than what many courts previously considered to be in the realm of "content based" discrimination. Before *Reed*, many courts held that a regulation is content based if the reason for the regulation was because the government disagreed with a particular message. *Reed* made clear that content based discrimination is much broader than that and extends to regulations based on the subject matter of the speech or topic of the speech.

One example of this change in the understanding of what is meant by "content based" is *Norton v. City of Springfield*, decided by the Seventh Circuit on August 7, 2015. *Norton v. City of Springfield*, 806 F.3d 411 (7 Cir. Aug. 7, 2015). Prior to *Reed*, the Seventh Circuit had affirmed the district court's holding that Springfield's anti-panhandling ordinance was content neutral. The ordinance prohibited oral requests for immediate donations of money in the city's historic district. The first time around, the Seventh Circuit had said:

> The Court has classified two kinds of regulations as content-based. One is regulation that restricts speech because of the ideas it conveys. The other is regulation that restricts speech because the government disapproves of its message. It is hard to see an anti-panhandling ordinance as entailing either kind of discrimination.

Id. at 412 (citing *Otterson v. City of Springfield*, 768 F. 3d 713, 717 (2014)). The court went on to conclude that this regulation discriminated based on subject matter, not viewpoint, and therefore was *not* content based, and therefore strict scrutiny should not apply. *Id.*

On a petition for re-hearing, following *Reed*, the Seventh Circuit changed course. Judge Easterbrook said that the Seventh Circuit had previously followed the approach taken by Justice Kagan in her dissenting opinion in *Reed*, that a law is not content based if it does not suggest that the government is trying to discriminate against unpopular ideas. Judge Easterbrook wrote the opinion and explained: "The majority opinion in *Reed* effectively abolishes any distinction between content regulation and subject-matter regulation. Any law distinguishing one kind of speech from another by reference to its meaning now requires a compelling justification." *Id.* The court therefore found the panhandling ordinance to be unconstitutional. *Id.* at 413.

Reed made clear that courts will employ a *two*-step analysis to determine whether a regulation is content based. First, courts will ask whether the regulation is content based on its face – whether it draws distinctions based on the message conveyed. This could be by topic, subject matter, idea, or message expressed. Or is the discrimination more subtle and distinguishing based on the "function or purpose" of the message? If so, strict scrutiny applies. The court has no need to even consider the government's justifications or purposes for enacting the regulation. It does not matter.

Second, if the law is not content based on its face, courts will *then* look at the reason for the regulation. Was it adopted by the government because the government disagreed with the content? If yes, strict scrutiny applies.

Under *Reed*, "a speech regulation targeted at specific subject matter is content based even if it does not discriminate among viewpoints within that subject matter." 135 S. Ct. at 2230. As

a shortcut, if you have to consider the content of the sign to see if the regulation applies to it, the regulation is content based. The *Reed* Court held, "A law that is content based on its face is subject to strict scrutiny regardless of the government's benign motive, content-neutral justification, or lack of 'animus toward the ideas contained' in the regulated speech." *Id.* at 2228. The result is that many more regulations of speech are subject to strict scrutiny than they were in the past and will be struck down. This is exactly what has happened over the last 10 months following the Supreme Court's issuance of this decision.

Importantly, because *Reed* defined what constitutes a "content based" regulation of speech, its reach extends beyond just regulation of signs, which was the particular type of regulation at issue in *Reed*. It extends to all regulation of speech. Thus, not only have we seen municipal signage regulations being struck down, and signage regulations being revised, in light of *Reed*, but also courts are striking down content based regulations of other forms of speech.

Reed has already been applied to regulation of social media postings and Internet communications. For example, in *Rideout v. Gardner*, 3 F. Supp. 3d 218 (D.N.H. 2015), the New Hampshire district court struck down New Hampshire's law that prohibited voters from taking and making public digital images or photos of completed ballots. The purpose was to prevent these images of completed ballots from being posted online, and the given reason for the law was to prevent voter coercion. *Id.* at 223-24. Because the law restricted certain speech based on its subject matter, it was content based and the court applied strict scrutiny. *Id.* at 229. The court said that the state's purported interest of preventing voter coercion was "compelling in the abstract," but it was not actually compelling because the state lacked evidence supporting that this was a real concern. *Id.* at 231. The court said that "the mere assertion of such interests

cannot sustain a content-based speech restriction. . . . For an interest to be sufficiently compelling, the state must demonstrate that it addresses an actual problem." *Id.*

The district court went on to find that neither the legislative history nor the evidentiary record provided any support for the argument that the state has an "actual or imminent problem with images of completed ballots being used to facilitate either vote buying or voter coercion." *Id.* at 232. There was just a third-hand mention of one incident of vote buying in 2012. Plaintiffs presented evidence that there were no complaints of vote buying since 1976. *Id.*

The court also found that even if there was a compelling government interest, the law was not narrowly tailored. *Id.* at 233. It was not the least restrictive means to obtain the stated objective. *Id.* at 234. It was over-inclusive because it would apply to people merely wanting to make a political point and not coerce voters, and people who would want to buy or coerce votes would likely not blatantly do so in this manner of posting completed ballots online. *Id.* The court also noted that under both federal and state law, it was already illegal to engage in voter coercion or to buy votes. An easy, much less restrictive means of achieving the stated objective would be to make it illegal to post online an image of a completed ballot in connection with a voter coercion scheme. *Id.* at 235. Thus, if the target of the regulation is already illegal, or could be made illegal in a manner that is less restrictive, it is not going to be narrowly tailored and should not survive strict scrutiny.

The line between what is considered regulation of speech versus regulation of conduct is not always clear in the context of Internet and social media regulations. In *State v. Packingham*, 777 S.E.2d 738 (N.C. 2015), *petition for cert. filed*, No. 15-1194 (Mar. 21, 2016), the North Carolina Supreme Court upheld a statute banning registered sex offenders' use of commercial social networking websites accessible to minors. The court found that this was a regulation of

conduct, not speech, and it was content neutral because it applied regardless of the type of speech used. *Id.* at 386-87. The court explained, "Although the statute may impose an incidental burden on the ability of registered sex offenders to engage in speech on the Internet, '[a] regulation that serves purposes unrelated to the content of expression is deemed neutral, even if it has an incidental effect on some speakers or messages but not others.'" *Id.* at 386 (quoting *Ward v. Rock Against Racism*, 491 U.S. 781, 791 (1989)).

The court held that the law was narrowly tailored to serve a substantial government interest, prohibiting registered sex offenders from accessing only websites that gave them the opportunity to gather information about minors, as the law left ample alternative channels of communications available including "text messages, FaceTime, electronic mail, traditional mail, and phone calls." *Id.* at 390-91. In addition, as the law was applied to this particular defendant, who had posted a statement on his Facebook page praising God because he had a ticket dismissed, was also constitutional. In doing so, however, the court noted that "[i]f merely 'liking' a post on Facebook.com is speech protected by the First Amendment, we have no doubt that posting a message on that site falls within this category as well. Thus, the statutory restrictions on defendant's right to speech on Facebook, while incidental, are not trivial." *Id.* at 392-93. A petition for certiorari to the U.S. Supreme Court was filed on March 21, 2016.

Demonstrating how difficult it can be to determine whether regulation of Internet communications constitutes regulation of conduct or speech, the U.S. District Court for the Middle District of Louisiana recently enjoined enforcement of a similar Louisiana statute on First Amendment grounds. In *Garden Dist. Book Shop, Inc. v. Stewart*, 2016 U.S. Dist. LEXIS 57623 (E.D. La. April 29, 2016), plaintiffs filed a motion for a preliminary injunction to enjoin the enforcement of Louisiana's H.B. 153, arguing that this law was unconstitutional because it

criminalizes the publication of "material harmful to minors" on the Internet by any person or entity in Louisiana. *Id.* at *6.[1] The court followed the Supreme Court's analysis in *Reno v. ACLU* and subsequent cases on regulating Internet content that is harmful to minors and found that the law was a content based restriction on speech and therefore presumptively unconstitutional unless the law passes strict scrutiny. *Id.* at *14-15. The court found that the plaintiffs were likely to succeed on the merits because there was a less restrictive alternative that was equally effective—content filtering. *Id.* at *19-20. The court also noted that the law was not very effective at achieving its purpose of protecting minors because it covered only Internet content uploaded in Louisiana after the law was enacted; thus, minors could still access Internet content uploaded outside of Louisiana or before the law's passage. *Id.* In addition, certain key terms in the law were vague and undefined, including what it means to "publish" material under the law, making the law overly broad and likely to chill free speech. *Id.* at *22 ("The ill-defined

[1] The pertinent parts of § 14:91.14 read as follows:

> (A)(1) Any person or entity in Louisiana that publishes material harmful to minors on the Internet shall, prior to permitting access to the material, require any person attempting to access the material to electronically acknowledge and attest that the person seeking to access the material is eighteen years of age or older.
>
> (2) The failure to comply with the provisions of Paragraph (1) of this Subsection shall constitute the unlawful distribution of material harmful to minors through the Internet.
>
> (3) If a person or entity in Louisiana publishes material harmful to minors on the Internet and complies with the provisions of Paragraph (1) of this Subsection, the person or entity shall not be held liable under the provisions of this Section if the person seeking to access the material is under the age of eighteen and falsely acknowledges and attests that he is eighteen years of age or older.
> . . .
> (B)(2) "Material harmful to minors" is defined as any digital image, photograph, or video which exploits, is devoted to or principally consists of, descriptions or depictions of illicit sex or sexual immorality for commercial gain, and when the trier of fact determines that each of the following applies:
>
> (a) The material incites or appeals to or is designed to incite or appeal to the prurient, shameful, or morbid interest of minors.
> (b) The material is offensive to the average adult applying contemporary community standards with respect to what is suitable for minors.
> (c) The material taken as a whole lacks serious literary, artistic, political, or scientific value for minors.

LA. STAT. ANN. § 14:91.14(A), (B).

terms in § 14:91.14 do not adequately notify individuals and businesses in Louisiana of the conduct it prohibits, which creates a chilling effect on free speech. For example, despite the array of definitions in Section (B) of the statute, it does not define 'for commercial gain' or 'publish.'").

The *Stewart* case involved a law that banned any person from "publishing" certain materials on the Internet, while the *Packingham* case involved a statute that prohibited certain people (registered sex offenders) from accessing certain social networking websites. The court in *Stewart* held that the law was a content based regulation of speech—and the law applied to the type of material uploaded (*i.e.*, communicated). The law in *Packingham*, on the other hand, was found to regulate conduct, not speech, as it regulated certain people's access to online forums (and was a content neutral regulation). Thus, regulating access to social media forums may be more likely upheld in the face of First Amendment challenges than regulating online postings, even though the former may actually constitute a broader restriction on online activities. Prohibiting access is more likely to be content neutral, in which case a lower standard of review would apply.

Apart from regulating Internet content, another important issue related to government's use and control of electronic information is the extent to which the government can compel access to electronic information for law enforcement purposes. The All Writs Act ("AWA") is a long-standing law in the United States that stems from the Judiciary Act of 1789, and although it has historically been used sparingly, Dimitri D. Portnoi, *Resorting to Extraordinary Writs*, 83 N.Y.U. LAW REV. 293, 295 (2008), it has been relied upon by the government to compel assistance with investigations and law enforcement. The AWA is intended to function as a "gap-filler," to fill gaps left in statutes as necessary. Brian M. Hoffstadt, *Common-Law Writs and*

Federal Common Lawmaking on Collateral Review, 96 NW. U. L. REV. 1413, 1460-61 (2002) (quoting *United States v. Valdez-Pacheco*, 237 F.3d 1077, 1079 (9th Cir. 2001)). While the judiciary's discretion under the AWA has historically been exercised sparingly, the courts generally apply the AWA when certain factors are met: (a) there are no alternative avenues to obtain the same relief; (b) there is an independent-basis for subject matter jurisdiction; and (c) "the writ is necessary or appropriate in aid of that jurisdiction." Portnoi, 83 N.Y.U. LAW REV. at 299. In addition, "the form of the injunction should conform to the usages and principles of law." *Id.* The Eleventh Circuit has held that, unlike a request for a traditional injunction, there is no requirement to state a claim in order to obtain an AWA injunction. Rather, it may be granted whenever it is "calculated in [the court's] sound judgment to achieve the ends of justice entrusted to it." *Klay v. United Healthgroup, Inc.*, 376 F.3d 1092, 1100 (11th Cir. 2004).

"[C]ourts have significant flexibility in exercising their authority under the Act." *United States v. Catoggio*, 698 F.3d 64, 67 (2d Cir. 2012). Pursuant to the AWA, courts have the power, "in aid of a valid warrant, to order a third party to provide nonburdensome technical assistance to law enforcement officers." *Plum Creek Lumber Co. v. Hutton*, 608 F.2d 1283, 1289 (9th Cir. 1979) (citing *United States v. New York Telephone Co.*, 434 U.S. 159 (1977)). The U.S. Supreme Court has upheld courts' authority under the AWA to issue orders to third parties to aid in the execution of search warrants, holding:

> The power conferred by the Act extends, under appropriate circumstances, to persons who, though not parties to the original action or engaged in wrongdoing, are in a position to frustrate the implementation of a court order or the proper administration of justice . . . and encompasses even those who have not taken any affirmative action to hinder justice.

434 U.S. at 174 (upholding order requiring New York Telephone Company to assist the government in installing a pen register, a device that records outgoing numbers dialed on a

phone, pursuant to a warrant). The Supreme Court held that the courts' authority "is not limited to tangible items but is sufficiently flexible to include within its scope electronic intrusions authorized upon a finding of probable cause." *Id.* at 169. Various types of compelled law enforcement have been upheld under the AWA including compelling a phone company to trace telephone calls, requiring a manufacturer to attempt to assist in accessing a cell phone's image files, and ordering a landlord to provide access to security camera videotapes.

Compelled speech is allowed under certain circumstances. For example, the government may require nutrition labels or disclosures in certain advertising. *See Zauderer v. Office of Disciplinary Counsel*, 471 U.S. 626, 651 (1985) (holding that a requirement that the purveyor of a good or service disclose factual information is constitutional if the requirement is not unduly burdensome and is "reasonably related to the State's interest in preventing deception of consumers."). The Supreme Court has also held that compelled speech protections do not apply to "essential operations of government" such "as in the case of compulsion to give evidence in court." *W.V. Bd. of Ed. v. Barnette*, 319 U.S. 624, 645 (1943) (Murphy, J., concurring). In addition, courts have held that where there is no audience, compelled speech protections do not apply or are much weaker. *See Full Value Advisors, LLC v. S.E.C.*, 633 F.3d 1101, 1108-09 (D.C. Cir. 2011); *United States v. Sindel*, 53 F.3d 874, 878 (8th Cir. 1995).

The robustness of First Amendment protections can be contrasted with the lack of a specific, well-defined right to privacy in the U.S. Constitution. As in many cases, it might be preferable for Congress to clarify the issue and pass a law addressing the important questions of how to balance the government's need to enforce its laws and protect the public with individual privacy and free speech concerns. However, unfortunately, the American legislative structure is designed to operate very slowly, and it has suffered from extreme gridlock in recent years, which

only appears to be tightening. Until then, we must rely on the judiciary to address these questions. *See generally* JOHN MARSHALL, THE SUPREME COURT IN AMERICAN HISTORY (1965) ("It is emphatically the province and duty of the judicial department to say what the law is.").

B. International Approaches to Balancing Law Enforcement and Privacy

If a foreign government wanted information from a U.S. telecommunications company or internet service provider ("ISP") in the U.S., it would have to follow the U.S. legal process, either pursuant to a Mutual Legal Assistance Treaty ("MLAT"), through which process the U.S. executive branch would determine whether the request was proper, or a letter rogatory, which would require a federal court to decide the request. Report of the Manhattan District Attorney's Office on Smartphone Encryption and Public Safety, at 9 (Nov. 2015), https://cyber.law.harvard.edu/pubrelease/dont-panic/DA_Report_Smartphone_Encryption_Public_Safety_11182015.pdf. Aside from these procedural issues, from a substantive standpoint, certain countries are not waiting for the U.S. to figure out how it will choose to balance the sometimes competing interests between law enforcement and privacy or free speech rights and are considering or passing laws authorizing government obtainment of electronic data in their jurisdictions.

In 2015, China passed a new counterterrorism bill that requires telecommunications operators and ISPs to give technical support and assistance to national security authorities for purposes of preventing and investigating terrorist activities. Tian Shaohui, "Provisions of China's Counterterrorism Bill Inspired by Foreign Laws," Xinhuanet (Dec. 27, 2015), http://news.xinhuanet.com/english/2015-12/27/c_134955978.htm. This includes assistance with decryption of devices if requested by law enforcement authorities, but does not require companies to install backdoors into security features. *Id.*; Ben Blanchard, "China Passes

Controversial Counter-Terrorism Law," Reuters (Dec. 28, 2015), http://www.reuters.com/article/us-china-security-idUSKBN0UA07220151228; Counter-Terrorism Law of the People's Republic of China, Ch. 3, Art. 18 (Dec. 27, 2015), *available at* http://chinalawtranslate.com/%E5%8F%8D%E6%81%90%E6%80%96%E4%B8%BB%E4%B9%89%E6%B3%95-%EF%BC%882015%EF%BC%89/?lang=en#_Toc439054064 ("Telecommunications operators and internet service providers shall provide technical interfaces, decryption and other technical support assistance to public security organs and state security organs conducting prevention and investigation of terrorist activities in accordance with law."). Failure to comply with the law could result in fines of about $30,000-$75,000 or 5-15 days of imprisonment. Tian Shaohui, "Provisions of China's Counterterrorism Bill Inspired by Foreign Laws," Xinhuanet (Dec. 27, 2015), http://news.xinhuanet.com/english/2015-12/27/c_134955978.htm.

The law broadly defines "terrorism" as: "propositions and actions that create social panic, endanger public safety, violate person and property, or coerce national organs or international organizations, through methods such violence, destruction, intimidation, so as to achieve their political, ideological, or other objectives." Counter-Terrorism Law of the People's Republic of China, Ch. 1, Art. 3 (Dec. 27, 2015), *available at* http://chinalawtranslate.com/%E5%8F%8D%E6%81%90%E6%80%96%E4%B8%BB%E4%B9%89%E6%B3%95-%EF%BC%882015%EF%BC%89/?lang=en#_Toc439054064. The law also requires that telecommunications operators and ISPs shall "put into practice network security systems and information content monitoring systems, technical prevention and safety measures, to avoid the dissemination of information with terrorist or extremist content." *Id.*, Ch. 3, Art. 19. In addition, "[w]here information with terrorist or extremist content is discovered, its

dissemination shall immediately be halted, relevant records shall be saved, and the relevant information deleted, and a report made to public security organs or to relevant departments." *Id.* Thus, the law compels all telecommunications operators and ISPs to take these actions rather than impose an interim step, such as a warrant request, to determine on a case-by-case basis whether the actions are reasonable and justified.

In 2015, British Prime Minister David Cameron said that his government must have access to private communications in order to protect the public: "[T]he question is are we going to allow a means of communications which it simply isn't possible to read. My answer to that question is: no, we must not. The first duty of my government is to keep our country safe." Report of the Manhattan District Attorney's Office on Smartphone Encryption and Public Safety, at 16 (Nov. 2015), https://cyber.law.harvard.edu/pubrelease/dont-panic/DA_Report_Smartphone_Encryption_Public_Safety_11182015.pdf. In June 2015, before Parliament, he stated:

> We have always been able, on the authority of the home secretary, to sign a warrant and intercept a phone call, a mobile phone call or other media communications, but the question we must ask ourselves is whether, as technology develops, we are content to leave a safe space—a new means of communication—for terrorists to communicate with each other. My answer is no, we should not be, which means that we must look at all the new media being produced and ensure that, in every case, we are able, in extremis and on the signature of a warrant, to get to the bottom of what is going on.

Id. at 17. The United Kingdom is currently considering the draft Investigatory Powers Bill, which would, among other things, create an Investigatory Powers Commission ("IPC") to oversee the collection of data and interception of communications. *See* Draft Investigatory Powers Bill, at 5, ¶ 75 & Ch. 1 (Nov. 2015), https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/473770/Draft_Inv

estigatory_Powers_Bill.pdf. The IPC would include a judge, who would review warrants for accessing communications and electronic devices. It states that where a Judicial Commissioner other than the IPC "refuses to approve a decision to issue a warrant under this Chapter, the person who made that decision may ask the IPC to decide whether to approve the decision to issue the warrant." *Id.*, Ch. 1, ¶ 19(5). It would also require communication service providers to assist with targeted interception of data and communications in relation to investigations. *Id.* at Ch. 2, ¶ 33. The bill provides for the interception of communications pursuant to requests made in accordance with relevant international agreements. *Id.* at Ch. 2, ¶ 39.

Europe is not unified on how to balance the issues of data privacy and intelligence gathering. For example, Hungary has suggested making encryption software illegal. Thorsten Benner and Mirko Hohmann, "How Europe Can Get Encryption Right: Consensus on Data Privacy and Intelligence Sharing on the Continent Will Be Crucial to Its Counter-Terrorism Efforts," Politico (Apr. 13, 2016), http://www.politico.eu/article/how-europe-can-get-encryption-right-data-protection-privacy-counter-terrorism-technology/. France is considering legislation that would fine tech companies and their executives that fail to decrypt user data (the fine would be $350,000 euros and five years of imprisonment) or who fail to design their own encryption. *Id.*; Daniel Severson, "The World's Not Waiting for California: France Moves to Enforce Decryption," Lawfare (Mar. 7, 2016), https://www.lawfareblog.com/worlds-not-waiting-california-france-moves-enforce-decryption; Proposed Bill on Combatting Organized Crime, Terrorism, and Related Financing and Improving the Efficiency and Guarantees of Criminal Procedure, *available at* http://www.assemblee-nationale.fr/14/projets/pl3473.asp.

The United Nations is also looking at these important issues. Reports by the United Nations have found that court-ordered decryption does not necessarily violate international

human rights. The May 22, 2015 report by Prof. David Kaye, U.N. Human Rights Council Special Rapporteur, "The Promotion and Protection of the Right to Freedom of Opinion and Expression," states:

> Court-ordered decryption, subject to domestic and international law, may only be permissible when it results from transparent and publicly accessible laws applied solely on a targeted, case-by-case basis to individuals (i.e., not to a mass of people) and subject to judicial warrant and the protection of due process of individuals.

Report of the Manhattan District Attorney's Office on Smartphone Encryption and Public Safety, at 17-18 (Nov. 2015), https://cyber.law.harvard.edu/pubrelease/dont-panic/DA_Report_Smartphone_Encryption_Public_Safety_11182015.pdf. The U.N. Human Rights Council enunciated a three-part test to determine when a government can restrict encryption:

> 1) The government restriction must be provided for by law. That law must be "sufficiently accessible, clear and precise so that an individual may look to the law and ascertain who is authorized to conduct data surveillance and under what circumstances." The law also must provide strong procedural and judicial safeguards in order to protect individuals' due process rights.
>
> 2) The government restriction may be imposed to achieve a legitimate objective, i.e., to protect specified rights, including "rights or reputation of others; national security; public order; public health or morals."
>
> 3) The government must demonstrate that the restriction is both necessary and proportionate to the specific risk being addressed.

Id.

III. LATENT GOVERNMENT ABUSE OF THE INTERNET AND SOCIAL MEDIA

> "Censorship reflects a society's lack of confidence in itself. It is a hallmark of an authoritarian regime . . . ."

> —Supreme Court Justice Potter Stewart, dissenting *Ginzburg v. United States*, 383 U.S. 463, 498 (1966).

It is important to assess how the Internet and social media are being used around the world by civil servants. There are examples of governments and officials using advances in technology to hamper, or in ways that have the effect of hampering, democratic principles and freedoms rather than promote them. Some activities are much more discreet, and perhaps they therefore pose an even more dangerous threat to free speech, and freedom generally. Do we need free online forums for a democracy to function in 2016? I believe so. The United Nations Universal Declaration of Human Rights 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.

The U.S. Supreme Court has said that "[a]nonymity is a shield from the tyranny of the majority." *McIntyre v. Ohio Elections Commission*, 514 U.S. 334, 357 (1995) ("It thus exemplifies the purpose behind the Bill of Rights, and of the First Amendment in particular: to protect unpopular individuals from retaliation – and their ideas from suppression – at the hand of an intolerant society."). But what happens when those in power use anonymity as a tool to repress free speech, especially communications that challenge those in power?

The Internet can allow people to impact public opinion and to repress opinions while hiding and not revealing who is really writing or controlling the information. The Internet abused in this way can allow the government or certain officials to control public opinion discretely, sometimes with no one being able to point the finger at who is actually doing it. Government officials are also able to use the Internet to create personas on Facebook—for example, a positive, biased image of a "true" representative of the people. This occurs in

established democracies as well, but in weak democracies, where there is a lack of real journalism, freedom of the media, and freedom of speech and expression, and where unpopular views such as statements questioning the government are punished, such online presences can be extremely repressive, not just untruthful. This is a higher risk in countries that do not have strong freedom of speech protections or many public forums. The Internet and social media can therefore constitute a new type of retribution for unpopular opinions.

The Internet has enabled us to communicate globally, share and process information at an incredible rate, and learn about issues affecting people on the other side of the world almost instantly. However, at the risk of appearing to be an overly simplistic point, it is critical to remember that, particularly in countries that do not have a robust freedom of speech or much independent journalism, the Internet provides an avenue for oppressive governments to control or even create their nation's image, with a lack of accountability. For example, government officials can use the Internet to paint a picture of an environmentally "sustainable" or "green" nation and encourage investment from international organizations as a result, for purposes of supporting environmental conservation, while in reality not enforcing its own environmental laws, zoning regulations, or requirements for environmental impact assessments for proposed development; ignoring obligations under international environmental agreements; and approving environmentally destructive projects including at the expense of previously endorsed conservation efforts.

For example, even though a country has ratified the United Nations Convention on Biodiversity (1992), https://www.cbd.int/countries/?country=kn, and the Cartagena Convention (1983), http://www.cep.unep.org/cartagena-convention/text-of-the-cartagena-convention, and thereby has agreed to undertake measures to protect threatened and endangered species, it may

be routinely approving development without considering effects on habitats of such species or even requiring comprehensive environmental impact assessments. Or it is not making available to the public information related to proposed developments and therefore is not obtaining meaningful comments or participation from citizens. For countries that lack transparency and free speech, even if touting itself as democratic, the picture painted to the outside world may appear very different from reality.

This concern is not just for the world's "Top Ten" authoritarian governments; a country can appear democratic on the surface, but really be highly controlled and have a very limited online public forum. In my experience in working with local attorneys in a developing democracy, I have seen government officials abusing the Internet and social media, such as by blogging under a pen name to lash out at people standing up to the government or asserting claims against the government. I have witnessed citizens expressing fear of speaking out, signing a petition, or even attending a community meeting—fear of incurring difficulty in obtaining much-needed government benefits and services or employment. Such tactics are a type of tyrannical cyber-bullying. There might be no, or limited, accountability for such unscrupulous behavior. How can such oppressive control of social media be addressed? How can citizens' concerns be heard in such a restricted society?

Having news media and journalism is important for promoting the expression of ideas and public discourse. However, this is not often robust in a new or emerging democracy. Another important option is the courts. If the judiciary can remain independent and there are strong-willed lawyers and plaintiffs, cases can be brought and hopefully justice may be served. Especially in a country where there is very limited media—essentially no access to court filings or other "public" documents—and people are afraid to speak out because there will likely be

repercussions by those in power, the judicial route will be a long and steep road. It will take a long time for matters to be resolved and for information to circulate to the public. But if a case results in justice, it could plant much-needed seeds of faith that the system can be functional and just.

Another option is utilizing the Internet for faster promotion of free expression by cooperating with international organizations and individuals in other countries who can provide support and also shed light on repression occurring locally. While the Internet can be used by the government to monitor and repress expression of ideas, if individuals are collaborating with international organizations and sharing information abroad, this can chip away at the government's control over its image and what is being discussed publicly, as it cannot as easily punish entities and individuals abroad. In addition, international pressure and threats to credibility and reputations can be especially powerful for developing democracies that may appear to be more democratic—and *want* to appear that way—compared to how they actually function. International organizations and individuals abroad should be aware of their considerable potential to make a difference.

In addition, in today's world of electronic data and recordkeeping, important issues and challenges relating to access to justice arise. If the majority of people in a society communicate electronically, via email, cell phones, and downloading information from the Internet, is a state or local government agency substantially hindering access to public information by only providing hard copies of documents? What if court filings are not done electronically, but when a member of the public goes to court to ask for a copy of a filing, his or her request for a hard copy is denied? Providing access to public documents is extremely important for communities to function and develop and to have participatory democracy. The world of land use, for

example—how a community chooses to develop itself and plan for its future—depends on community participation to function. It is critical that stakeholders in the community be involved and have a voice in the planning process, from neighbors to developers, and from local businesses to concerned citizens and environmental groups. It is critical to demand enforcement of open records and freedom of information laws.

Beyond mere participation, what is really needed is *effective* engagement. Not only does information regarding public matters need to be made available (in my field, information related to planning as well as proposed and approved developments), but moreover, citizens' comments should actually be taken into account by the government. Otherwise the participation is meaningless. "Public participation should be fully incorporated into environmental assessment and decision-making processes, and it should be recognized by government agencies and other organizers of the processes as a requisite of effective action, not merely a formal procedural requirement." THOMAS DIETZ AND PAUL C. STERN, PUBLIC PARTICIPATION IN ENVIRONMENTAL ASSESSMENT AND DECISION MAKING, 226 (2008) [hereinafter PUBLIC PARTICIPATION]. The Internet and social media have immense potential to aid in achieving these democratic goals of meaningful civic participation, transparency, and accountability, but that potential has not yet been realized. United Nations Development Programme, *Reflections on Social Accountability: Catalyzing Democratic Governance to Accelerate Progress Towards the Millennium Development Goals*, at 2 (July 2013), http://www.undp.org/content/dam/undp/documents/partners/civil_society/2013_UNDP_Reflections-on-Social-Accountability_EN.pdf (listing and explaining these goals; explaining that "accountability" is "the obligation of power-holders to take responsibility for their actions."); DIETZ AND STERN, PUBLIC PARTICIPATION at 226; LeRoy Paddock, *Environmental*

Accountability and Public Involvement, 21 PACE ENV. L. REV. 243, 244 (2004) ("Earlier, more interactive and more 'authentic' public participation is a critical aspect of strengthening environmental accountability and assuring better environmental outcomes.").

These risks to democracy highlight the important and necessary role of the judiciary, and the need for the international community to take a collective interest in each other and learn about on-the-ground enforcement of international agreements, or lack thereof. Jane Jacobs, a Canadian and American journalist and thought leader on urban development, famously said that in order to make public areas safe,

> there must be eyes upon the street, eyes belonging to those we might call the natural proprietors of the street. The buildings on a street equipped to handle strangers and to insure the safety of both residents and strangers, must be oriented to the street. They cannot turn their backs or blank sides on it and leave it blind.

JANE JACOBS, THE DEATH AND LIFE OF GREAT AMERICAN CITIES (2002). In other words, in a public space, if people feel that others are watching, they will hold themselves to a higher standard and the public space will be safer as a result. This concept is applicable to enforcement of international legal obligations. The more that we can share information using the Internet and social media to inform others, and to indicate that people are interested, involved, and watching, the more that these tools can be used to increase accountability. Whether these tools will reach their full potential remains to be seen.

IV. CONCLUSION

Myriad unsettled issues related to government regulation or use of electronic information will undoubtedly continue to make their way through courts and legislatures around the globe. As advances in technology continue, new legal questions will inevitably arise. Where governmental abuse of the Internet and social media is latent and not being formally challenged,

international awareness and dialogue should be employed to the extent possible. A significant by-product of governments overstepping, especially without effective oversight such as from an independent judiciary—whether via overly broad regulations of online communications or government officials' repressive use of social media—is a pervasive mistrust of the entire system. A democratic system requires that people uphold and participate in it. This underscores the importance of the national, and, truly, global, debate on these issues. Whichever way a court or legislature comes out, if people see that a process was followed and interested parties have a full and fair opportunity to participate and be heard, the system will continue and will likely be stronger for it.

> The very problems that democratic change brings – social tension, heightened expectations, political unrest – are also strengths. Discord is a sign of progress afoot; unease is an indication that a society has let go of what it knows and is working out something better and new.
>
> -Sandra Day O'Connor