Intermediaries and Freedom of Expression

Hiram A. Meléndez-Juarbe*

I. INTERMEDIARIES AND THE RISK OF OVERENFORCEMENT

The days in which we thought of the digitally interconnected environment as absolutely exceptional, completely immune from governmental reach, are behind us.[1] It is unquestionable that our online activity is capable of being regulated because, as a practical matter, law and other forces have the power to structure the technological environment.[2]

To a large extent, this is so because the Internet is not an abstract entity—it depends on intermediary institutions that make communication possible and that are within reach of governments with conventional coercive mechanisms. Online activity is regulated by controlling these intermediaries— *connection intermediaries* (such as Internet Service Providers); *information intermediaries* (such as search engines); and *financial intermediaries* (like credit cards and PayPal),[3] among others.[4]

The role played by intermediaries in online regulation is vital. To the extent that governments pursue political objectives online (legitimate or not), individuals gradually become less interesting regulatory targets. Instead, entities that provide technological means for individual activity attract the most attention. After all, it will be easier and cheaper to go after a few institutions within a state's jurisdiction rather than pursuing thousands of hard to reach individuals dispersed around the planet.

In this context, one of the most effective ways to regulate via intermediaries is by subjecting them to (civil or criminal) liability for behavior in which their users or clients engage in. The objective of this strategy is to make these entities feel pressure in their pockets for potentially illegal activity of their clients and, in this way, use their technological resources to supervise or punish user activity (pursuant to the superior information and opportunity they have to do this, relative to governments or third parties).

---

* Associate Professor University of Puerto Rico Law School. BA, University of Puerto Rico 1997; JD, University of Puerto Rico 2000; LL.M., Harvard University 2002; LL.M., New York University 2008; JSD Candidate, New York University. Contact information at www.elplandehiram.org/write. Similar reflections were presented in a previous work for the Seminar in Latin America on Constitutional Law and Politics (SELA), june 2011, entitled Technopolitics and Copyright Regulation. I am indebted to Edgardo Canales and Marini Rodriguez, third year students at the University of Puerto Rico Law School, for their help translating this essay into English.

[1] Jonathon W. Penney, *Understanding the New Virtualist Paradigm*, Journal of Internet Law, Vol. 12, No. 8 (2009).

[2] LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE (1999).

[3] *See, eg*, Troy Wolverton, *N.Y. subpoenas PayPal over gambling,* http://news.cnet.com/N.Y.-subpoenas-PayPal-over-gambling/2100-1017_3-943533.html (July 12, 2002).

[4] JACK GOLDSMITH AND TIM WU, WHO CONTROLS THE INTERNET: ILLUSIONS OF A BORDERLESS WORD (2006).

But this behavior is not limited to the digital environment. Regulation through proxies is a common strategy, particularly with regard to expression.[5] Exposing intermediaries to liability (turning them into guardians or gatekeepers) in order to recruit their help in the enforcement of normative objectives happens when direct enforcement against wrongdoers would not dissuade the controversial conduct or where it is costly.

But the main risk behind this strategy is the likelihood of overenforcement. To the extent that intermediaries and users have divergent interests, a given intermediary will not necessarily take into account the value that the regulated activity has to the user. Instead, the intermediary will rationally behave so as to maximize its welfare, seeking to minimize its expected liability cost. In the end the problem is that, when balancing private liability costs against the private benefits of an intermediary's economic activity, in its self-interested conception of what constitutes wellbeing, the intermediary will not consider user's free speech interests (or the social interest in that the user engages in activity presumably connected to freedom of expression).

In this essay, I examine this strategy in the context of state regulation of copyright law, child pornography and privacy, dignity and honor affronts (such as defamation), and the potential impact that this kind of enforcement might have on freedom of speech. To that effect, and instead of developing detailed prescriptions about how to address the risk of overenforcement, I will outline some notes for defining a–theoretical and practical— research agenda so that we can help civil society forge sensible policy strategies. In all, I will put forth some points of departure to continue this conversation.

II. FREE SPEECH CONTEXTS

The first point of departure to bear in mind is this: regulatory efforts should only consider deploying legal mechanisms that are specifically tailored to distinct expressive contexts. That is, we must worry about applying one-size universal solutions to all kinds of contexts.

Protecting copyright online, preventing child pornography and avoiding abusive attacks against honor and private life are surely legitimate governmental interests in Latin America. But their regulation through intermediaries, however important, presents overenforcent risks that are impossible to ignore. This is why we must select legal regulatory mechanisms that, while attempting to address legitimate goals, minimize free speech erosion. But, and this is the rub, each of these expressive contexts presents unique free speech challenges. Because overenfocement might affect different free speech values according to the kind of problem being addressed (copyright, child pornography, honor), regulatory mechanisms should probably be different in each case.

Because intermediary liability rules should vary according to the kind of communicative act being targeted, we need precise substantive understandings on the social values present at each of these expressive contexts (what kind of defamation is tolerable, in what

[5] Seth Kreimer, *Censorship by Proxy- the First Amendment Internet Intermediaries and the Problem of the Weakest Link*, 155 U. PA. L. REV. 11 (2007). *See* NAACP v. Alabama ex rel. Patterson, 357 US 449 (1958) (invalidating a state requirement for Alabama's NAACP membership list); New York Times v. Sullivan, 376 US 254 (1964); Bantham Books v. Sullivan, 372 US 58 (1963).

circumstances authors interests should be overridden by free speech concerns, and why). In order to prescribe which are the most reasonable regulatory measures that would minimize overenforcement risks, we must first navigate through muddy waters and define those free speech values we want to protect in these contexts. And, in that process, make difficult judgment calls on extraordinarily hard issues.

In this sense, for example, it is necessary to understand what distinguishes those expressive interests of an unauthorized copyright user from the interests of someone expressing herself in ways that conceivably affect another's good name and honor. Are these individual interests similar? Seen from the other side of the coin, is the alleged harm suffered by an author whose work is used similar to the harm suffered by the defamed? As a next step we must ask, if these interests are not similar (those of the unauthorized user, the defamer, or the pornographer), then, do we need different kinds of regulations for those intermediaries that facilitate these conducts? In what way will they be different? Subsequent research should take these questions as points of departure systematically. Here I offer initial suggestions.

Clearly, free speech interests are different in each case and they are balanced against different collective and individual interests.

On one hand, expression that potentially affects someone's honor and private life could be limited by the social and individual interest in preserving those civility rules that create conditions for social cohesion, such as equal respect for human dignity.[6] Defamation law provides an example: the Inter-American constitutional regime allows limiting defamatory expression against private persons preserving those social norms, but makes liability harder for the case of governmental public figures (because of the value imposed given to participation in public discourse).[7] In any case, there is no magic rule to define with precision what constitutes an abusive attack against honor and reputation, although there will be powerful reasons to protect the expression in many cases (as in the case of public figures). Lack of certainty regarding what distinguishes protected from unprotected expression, generates in the intermediary the aforementioned risk of overenforcement; particularly when penalties are high, which conditions their cost-benefit analysis.

On the other hand, unauthorized use of works created by others (and protected by copyright law), ought not be demonized as "theft" or "piracy"; such use could be related to individual or collective interests tied to political or artistic expression. Unauthorized use could be part of what Fisher calls "semiotic democracy"[8]—decentralization of the power to give meaning to elements of our culture. These uses are highlighted today in the context of digital technologies since the material conditions for the production and manipulation of cultural products allow us to indentify ourselves and personally experiment with them, as active participants of cultural processes and not simply as

---

[6] See generally, ROBERT POST, CONSTITUTIONAL DOMAINS: DEMOCRACY, COMMUNITY AND MANAGEMENT (Harvard 1995); STEVEN HEYMAN, FREE SPEECH AND HUMAN DIGNITY (2008).

[7] Kimel v Argentina, Sentencia May 2, 2008, Inter-American Court of Human Rights, Paragraph 86.

[8] WILLIAM W. FISHER III, PROMISES TO KEEP: TECHNOLOGY, LAW AND THE FUTURE OF ENTERTAINMENT 30-31 (Stanford 2004)

passive consumers of information.[9] However, copyright balances these free speech interests with two other collective and individual concerns: (a) copyright (particularly author rights) is sometimes justified as morally deserved—resulting from the mixture of individual work with common resources and/or given the personal connection between the author and her work and (b) an interest in maximizing social welfare by giving enough incentives to information producers through the privatization of intellectual resources (while also limiting their rights to prevent deadweight loss and underuse).[10] And so, combining these competing interests is complex, contextual and indeterminate. It is not enough to merely allege that someone has an absolute property right over a work, without considering free speech interests that might be affected; but it is also insufficient to assert that an individual has an unqualified right to all kinds of unauthorized uses (ignoring the social and individual interests that justify the monopoly). Hence, we need normative criteria to help us strike these balances; criteria that will be different to those factors used in the context of dignity rights. For example, pertinent criteria here would be: the commercial or personal nature of the use or if the use is merely consumptive or productive—elements that have nothing to do with the other expression contexts here examined.

Finally, although free speech interests over sexually explicit material can be more controversial, it is difficult—if not impossible—to justify child pornography. What is difficult, in many cases, is to distinguish what is actually child pornography from other sexually explicit content. There are notorious cases in which employees of film development services have reported to the authorities people who submitted film with pictures of their children in contexts that—although technically could be interpreted as child pornography—are in fact everyday familial affairs recorded with no prurient interest whatsoever;[11] and cases in which adult models appear to be minors.[12] In these cases, we must examine those free speech interests underlying non-child pornography—interests that could be tied to individual autonomy and self-definition.

Each one of these free speech environments reflects distinct internal problems (and balances) generating ambiguity in determining which is exactly the conduct to avoid. This ambiguity (in some cases more than others) is a key factor in the before mentioned overenforcement risk: the risk that the intermediary, in order to avoid liability, will act against objectionable conduct but, along the way, affect socially valuable conduct or speech. Uncertainty as to whether the conduct facilitated by the intermediary is legal or not (and therefore uncertainty as to whether it is liable or not) will induce the intermediary to be more conservative about which conduct to allow. But the kind of ambiguity and the reasons for its existence will be different in each setting. And the intermediary liability regime we choose in the face of this uncertainty, will reflect an

---

[9] Yochai Benkler, *From Consumers to Users: Shifting the Deeper Structures of Regulation Toward Sustainable Commons and User Access*, 52 FED. COMM. L. J. 561 (2000).

[10] Hiram Meléndez Juarbe, *Tecnopolítica y Derechos de Autor,* disponible en http://www.law.yale.edu/documents/pdf/sela/SELA11_Melendez_PV_Sp_20110802.pdf

[11] ABC News, *Photo Labs Part of Fight Against Child Porn?*, http://abcnews.go.com/2020/story?id=132673, last visited September 19, 2011.

[12] Ashcroft v. Free Speech Coalition, 535 U.S. 234 (2002).

underlying value judgment about the free speech interests involved in each set of problems.

At bottom, the choice between mechanisms that expose the intermediary to liability to a greater or lesser degree will reflect an assessment of risk that considers the magnitude of overenforcement risks (that is, an underlying determination about the free speech values we want to protect and up to which point we want to protect them). Thus, if we care little about the risks involved in an intermediary's efforts to prevent the circulation of child pornography, maybe we could tolerate a kind of intermediary regulatory regime that imposes stronger policing duties than the ones we would tolerate for the copyright or privacy contexts. Overenforcement in these latter two contexts presents risks of political, artistic or cultural censorship that might not be present in the former context (or at least are present to a lesser degree). This substantive evaluation is, I believe, the first conceptual step we must take before proposing concrete solutions.

III. MODES OF REGULATION

In order to balance the diverse interests at play, within the various contexts, we can think of four chief regulatory modes by which the law typically addresses intermediaries.

First, we could structure a system of *absolute immunity* for intermediaries, as is the case in the United Sates through section 230 of the Communications Decency Act, dealing with intermediary liability for damages to dignity and reputation caused by third parties.[13] Although this alternative is strongly supported by various groups as necessary in order to promote public debate and innovation online,[14] it is nonetheless controversial and is highly criticized by those who prefer imposing on the intermediary *ex ante* or *ex post* duties.[15] In the end, this immunity regime reveals a strong substantive positive valuation of free speech interests at play (vis-à-vis privacy interests) with the consequence that any risk of overenforcement appears unreasonable.

Second, we could conceive a system of *strict liability* that attributes liability for reasons that have nothing to do with the intermediary's diligence or his awareness of the illicit act, forcing it to compensate damages caused by users of the service.[16] However, as Ruiz Gallardo and Lara Galvez point out, this does not seem to be the trend in Latin America,[17] and in my opinion, a regime of this character would heighten the risk of overprotection. In extreme cases, it would increase the expected liability cost of the intermediary to such degree that this expense would surpass any potential benefits derived from engaging in the economic activity, preventing the intermediary from offering the service in the first place.

---

[13] 47 USC § 230.
[14] See, for example, Zeran v. America Online, Inc., 129 F.3d 327 (4th Cir. 1997).
[15] SAUL LEVMORE & MARTHA NUSSBAUM, THE OFFENSIVE INTERNET: SPEECH, PRIVACY, AND REPUTATION (2011).
[16] See Claudio Ruiz Gallardo y J. Carlos Lara Gálvez, *Responsabilidad de los Proveedores de Servicios de Internet (ISPs) en relación con el ejercicio al derecho a la Libertad de Expresión en Latinoamérica*.
[17] *Ibid.*

Third, we could think of systems of *duty-based liability* by which the intermediary could be liable by fault or malice, for example, by breaching its duty to act diligently preventing wrongdoing or failing to act immediately after realizing and learning of the illicit action. Presently, this model seems to predominate in countries such as Argentina and Chile in privacy and reputation cases.[18]

Finally, the most commonly used system for protection of copyright in the various neighboring jurisdictions, as well as worldwide, is a *conditioned immunity* regime; where immunity is conditioned upon compliance with diverse obligations, some more worrisome than others. Thus, we can have "notice and takedown" regimes that recruit intermediaries in order to facilitate takedown of content after notification by an alleged copyright owner or after court notification (depending on the jurisdiction). In principle, such regimes are incorporated into regional free trade agreements such as the Trans-Pacific Partnership Agreement[19] and the Free Trade Agreement between Colombia and the United States,[20] the latter being the backbone for the recently proposed intermediary liability law in Colombian.[21] The devil, as they say, is in the details: we have to define what are the conditions intermediaries will have to comply with in order to receive immunity—what supervising duties will they have, should they behave as active policemen, for example, if the removal of content or the cancelation of user accounts is contemplated, and what types of legal or private procedures will be in place for prompting takedowns.[22]

On the other hand, during implementation of these regimes—particularly duty-based liability and conditioned immunity— we find mechanisms that impose diverse kinds of duties on intermediaries. Following Reinier Kraakman[23] and Jonathan Zittrain,[24] I suggest we consider two types of general methods: bouncers and chaperones.

Intermediaries behave as *bouncers* when they address unwanted behavior by blocking it, closing a door, refusing to have a relationship with the presumed wrongdoer. A gatekeeper of this nature will generally be able to keep out individuals, by complying with precise and narrow duties (like requesting identification to verify age before dispensing alcohol or, in the ISP context, blocking Internet access to users after judicial mandate, or taking down content after receiving a private notification).

Yet, when intermediaries detect and limit user activity during the course of continuous relationships, they act more like *chaperones*, and within that role they engage in complex monitoring activities that respond to duties that are more diffuse than those of a bouncer

---

[18] *Ibid.*
[19] See discussion in Ruiz Gallardo y Lara Gálvez, *Ibid.*
[20] See http://www.ustr.gov/trade-agreements/free-trade-agreements/colombia-fta/final-text
[21] See Carolina Botero, *Proyecto de Ley sobre infracciones al derecho de autor en Internet* (April 5, 2011) at http://www.karisma.org.co/carobotero/index.php/2011/04/05/proyecto-de-ley-sobre-infracciones-al-derecho-de-autor-en-internet/
[22] The Chilean law requires judicial intervention befote taking down content. Ley de Derechos de Autor de Chile, Ley 17336 2 de octubre 1970, según enmendada 4 de mayo de 2010, Ley 20435; available at http://www.leychile.cl/Navegar?idNorma=28933&idVersion=2010-05-04
[23] Reinier H. Kraakman, *Gatekeepers: The Anatomy of a Third-Party Enforcement Strategy*, 2 J. L. ECON. & ORG. 53 (1986).
[24] Jonathan Zittrain, *A History of Online Gatekeeping*, 19 HARV. J. L. & TECH. 253 (2006).

(for example, a duty of care triggering monitoring requirements, such as filtering). In many cases the law imposes duties creating chaperones and bouncers. In other instances, intermediaries' self-regulating behavior generates these regimes.

The question is whether in each of the different free speech contexts we have seen (copyright, child pornography and privacy) there are reasons to prefer strict liability, duty-based liability, or conditioned immunity and, within them, chaperone or bouncer regimes or if, on the other hand, there are reasons for not imposing any liability to the intermediary at all.

There are no simple answers to this query; yet, some factors should provide guidance.

(a) Primarily, and so that we can evaluate the risks associated with the intermediary's behavior, the weight society is willing to give to the user's conduct (its value in free speech terms).

(b) The cost of chaperone or bouncer measures, and how feasible it is for the intermediary to undertake that activity (monitoring, filtering, etc).

(c) Crucially, the degree of certainty or uncertainty as to whether the user's conduct is constitutionally protected.

(d) The degree of ambiguity regarding the duties imposed on the chaperone or bouncer.

(e) The costs to the intermediary if found liable.

(f) The impact of the intermediary's supervision over other valuable interests, such as anonymity and privacy.

The harder it is to determine if a user's behavior is illegal or constitutionally protected, the higher the liability cost to the intermediary, and the more we value users' expressive—yet vulnerable—conduct, then the higher is the risk of overenforcing the state's interest in detriment of important expressive values.

Of all these factors, and given its importance for the intermediary's cost-benefit analysis, I will delve on the third one: the degree of uncertainty as to whether the behavior is constitutionally protected or, if on the other hand, it can be outlawed.

IV. THE ROLE OF AMBIGUITY

Notice the role that ambiguity plays in all of this. The risk of overenforcement does not depend exclusively on a factual scenario in which the intermediary has special and precise duties (such as in notice and takedown regimes), or active duties of identifying and reporting wrongdoers.

As mentioned before, a system of strict liability presents risks because it is hard for an intermediary to know *ex ante* if the conduct it facilitates is legal or not. But the problem is not limited to that kind of liability. A system of duty-based liability (like a negligence standard), joined to uncertainty as to the reach of constitutional protections, is enough to

materialize overenforcement risks.

Since it is difficult to differentiate the injurious form the constitutionally protected, any notification by an allegedly affected individual will suffice to intimidate the intermediary; the mere possibility of an expensive legal trial is enough to generate overprotection.

For example, Argentinean[25] and Chilean[26] cases relating to dignity harms suggest a negligence (non-strict) liability standard that, in practice, imposes a duty of constant supervision—to the extent that the ISP's duties are triggered as soon as it has knowledge (or should have knowledge) of the existence of harmful activity. In this sense, the negligence standard imposes on the intermediary —initially—a chaperone role. In Chile, this system produces a duty (in the first instance of the *Entel* case) to take necessary measures to identify the users responsible for defamatory expressions even though, on appeal, the impact of this duty is mitigated by the equally ambiguous principle of "freedom of information circulating in the net". However, this duty of reasonable care quickly turns into a duty to take action *ex post* following any notification. Once informed of the alleged illicit act, this notification (however deficient) transforms the intermediary (from a chaperone with a duty of care and supervision) into a bouncer to take immediate blocking action because it is impossible (or costly) to evaluate *ex ante* the legitimacy of the claim (due to the difficulty in distinguishing the legitimate from the illegitimate speech claim).

This way, whenever there is ambiguity, a chaperone type system in a duty-based liability regime has the potential of turning into a *de facto* bouncer system similar to a notice and takedown regime: any notification is sufficient to configure the subjective element of knowledge, resulting in an immediate takedown of content.

Depending on our valuation of the constitutional interests at play, these risks may be unacceptable. In other cases, when ambiguity in the illegality of the conduct is reduced, and the risks against free speech interests are more tolerable, a bouncer style system could be suitable; such as possibly with child pornography. In fact, this is how it works in Brazil, where a system of official notification and takedown is in place.[27]

But in the majority of cases there is little opportunity to establish clear and precise lines

---

[25] Cámara Nacional de Apelaciones en lo Civil, sala D, Expte. Nº 99.620/2006 "D. C. V. c/ Yahoo de Argentina SRL y otros/ Daños y Perjuicios" Recurso Nº 541.482. Juzgado Nº 75. See Discussion in this Volume, Claudio Ruiz Gallardo y J. Carlos Lara Gálvez, Responsabilidad de los Proveedores de Servicios de Internet (ISPs) en relación con el ejercicio al derecho a la Libertad de Expresión en Latinoamérica.

[26] Corte de Apelaciones de Concepción, Verdict on appeal, causa Paulina Fuentes Almendra y otro con ENTEL S.A.; Carmen Gloria Yáñez Vargas, rol 1223-2003, December 21, 2007 judgment. See Discussion in this Volume, Claudio Ruiz Gallardo y J. Carlos Lara Gálvez, Responsabilidad de los Proveedores de Servicios de Internet (ISPs) en relación con el ejercicio al derecho a la Libertad de Expresión en Latinoamérica.

[27] Estatuto de la Niñez, article 241-A (Inciso II). See discussion in this Volume, Claudio Ruiz Gallardo y J. Carlos Lara Gálvez, Responsabilidad de los Proveedores de Servicios de Internet (ISPs) en relación con el ejercicio al derecho a la Libertad de Expresión en Latinoamérica.

for low-cost bouncer regimes, or to envision chaperone systems that do not generate incentives for overprotection. Take, for example, notice and takedown copyright systems (for hosting services): precisely because it is difficult to determine when property rights are infringed, taking down content immediately is the only reasonable option for an intermediary. This predictable reaction from these intermediaries creates opportunities for perverse strategic action from right holders as it creates incentives to submit false notifications: for example, a study found that 30% of takedown requests where based on weak legal arguments and that very few users take advantage of the counter-notification procedure provided by law.[28] Furthermore, it has been found that right holders regularly send takedown notices to intermediaries about supposed participants in peer-to-peer sites even when these users do not download or share content at all.[29]

In this sense, at least in defamation and copyright cases, because of inherent substantive ambiguity within these free speech contexts, any system that delegates (directly or indirectly) supervision to intermediaries (whose interests differ from users') would be problematic. [30]

If ambiguity is a big part of the problem and delegating policing functions to intermediaries is problematic, then, we generally have two viable options. We either (a) absolutely immunize ISPs from liability (as with online defamation in the United States) or (b) we establish disambiguation mechanisms capable of distinguishing between constitutionally protected activity and illegal one, by delegating this task into organisms able to consider users' liberty interests (such as courts or other administrative bodies), mediated by appropriate procedural guarantees (such as the Chilean copyright law which requires judicial intervention for content takedown).[31]

V. TOWARDS A REFORMED CONDITIONAL IMMUNITY MODEL

It is clear that at least two of the four types of regulation mentioned above (absolute immunity, conditional immunity and strict and duty-based liability), have disfavored elements under conditions of ambiguity. On one hand, a strict liability system presents high risks of overprotection; on the other, a duty-based liability system will likely turn into a notice and takedown model whenever a notification is presented whenever there is

---

[28] Jennifer Urban, *Efficient Process or 'Chilling Effects'? Takedown Notices under Section 512 of the Digital Millennium Copyright Act*, 22 SANTA CLARA COMP. & HIGH TECH L. JOURNAL 621 (2006).

[29] Michael Piatek, Tadayoshi Kohno & Arvind Krishnamurthy, *Challenges and Directions for Monitoring P2p File Sharing Networks -or- Why My Printer Received a DMCA Takedown Notice Why My Printer Received a DMCA Takedown Notice*, University of Washington Technical Report, UW-CSE-08-06-01. http://dmca.cs.washington.edu/ (In two separate studies in 2007 and 2008 investigators introduced "users" with University of Washington IP addresses to monitor traffic. Even though those "users" did not download files, more than 400 notifications were received).

[30] In the USA, even for ISPs that do not engage in hosting, and whose immunity is almost guaranteed, recently the chief companies (AT&T, Cablevision, Comcast, Time Warner Cable & Verizon) established a system of private supervision consisting of "copyright alerts" and "mitigation measures", such as reducing the connection speed, or the suspension of the service—measures that could potentially affect freedom of speech. http://www.copyrightinformation.org/alerts

[31] Ley de Derechos de Autor de Chile, Ley 17336 2 de octubre 1970, según enmendada 4 de mayo de 2010, Ley 20435.

ambiguity (the majority of cases).

In light of this, we are left with absolute and conditional immunity models. The former, as suggested before, could be convenient only if the risks of an erroneous determination are too high with respect to freedom of speech interests, as deemed in the United States with section 230 of the Communications Decency Act, which absolutely exempts intermediaries from liability for third party defamation. I favor this alternative for defamation and abusive dignity harms since the risks of undermining valuable speech is high. However, this conclusion will depend substantive balances made in Latin America with respect to sometimes competing political values behind free speech interests and human dignity; a balance for which their is no universal consensus.

If absolute immunity is not available, an independent disambiguation mechanism would be necessary to avoid overprotection problems that emerge when we delegate supervision of online activity to intermediaries. In this process, the judiciary has a vertebral role to play. After all, if individual rights are involved and if there's a risk of takedowns affecting freedom of expression, then courts should be the ones balancing governmental interests behind regulation with individual rights.

The conditional immunity model (mediated by judicial intervention previous to any takedown of content) could be modified for these purposes, but only if coupled with processes respectful of individual rights, like privacy, due process of law and freedom of information. Some reform models have been proposed and they emphasize, among other things, giving users a real opportunity to respond to claims against them (prior to content takedown) and the imposition of stiffer sanctions to those who abuse the system by filing deficient claims.[32]

VI. CONCLUSION

In Latin America and in the rest of the world we should realize that, even when information technologies have impressive free speech potential, this potential is coupled with equally impressive opportunities for effective state and private control.

Understanding their reach—both the possibilities of expression and potential regulation— is essential for exercising our civil liberties on the net. Allowing ourselves to be lured by the promise of new technologies, and receiving them uncritically, entrenches in the *status quo* contemporary restrictions on our rights that are enforced through these technologies we consume. But we should also reject the attitude that assumes the technological environment as overwhelming and dystopian and, with that, refuse reasonable efforts to regulate our online behavior.

Crucially, it is important to understand how we benefit from the liberating potential that

[32] See Dena Chen, Musetta Durkee, Jared Friend, and Jennifer Urban, Copyright Reform Act: Updating 17 USC § 512's Notice and Takedown Procedure for Innovators, Creators, and Consumers (2011), available on http://www.publicknowledge.org/files/docs/cranoticetakedown.pdf; Wendy Seltzer, Free Speech Unmoored in Copyright's Safe Harbor: Chilling Effects of the DMCA on the First Amendment, 24 HARV. J.L. & TECH 171 (2010).

digitally networked technologies bring about, while at the same time addressing serious concerns to regulate online conduct in order to promote important social objectives like copyright, child pornography prevention and attacks against dignity, honor and privacy. This balance should guide us as we propose legal and policy reform in an interconnected digital environment.