Telecommunications Policy ▮ (▮▮▮▮) ▮▮▮–▮▮▮

Contents lists available at ScienceDirect

Telecommunications Policy

URL: www.elsevier.com/locate/telpol

Comment Paper

Hyper-transparency and social control: Social media as magnets for regulation ☆

Milton L. Mueller

Georgia Institute of Technology, School of Public Policy, 685 Cherry Street, DM Smith Rm 302, Atlanta, GA 30332, USA

This paper explores the interactions between social media governance, public perception and public discourse. Social networking platforms are Internet intermediaries; their legal responsibility for the actions taken by their users is an important topic in Internet governance. This paper takes a new and somewhat unusual approach to that problem. It examines the association of Internet intermediaries with certain kinds of activities, both good and bad, and how that creates powerful but sometimes irrational normative pressures on them. This happens, I argue, because social media applications make human interactions hyper-transparent. The mundane human activities that are coordinated through social media, including negative things like bullying, gossip, rioting and illicit liaisons, have always existed. In the past, these individualized or group interactions were not as visible or accessible to society as a whole. As these activities are aggregated into large-scale, public commercial platforms, however, they become highly visible to the public and generate storable, searchable records.

The new transparency and objectification of social interaction in social networking applications has powerful effects on the dialogue about control of communications. It lends itself to the idea that social media causes the problems revealed and that society can be altered or engineered by meddling with the intermediaries who facilitate the targeted activities. Hyper-transparency generates what I call the *fallacy of displaced control*. Society responds to aberrant behavior revealed through social media by generating pressures to regulate the intermediaries, instead of identifying and punishing the individuals responsible for the bad acts. There is a tendency to go after the public manifestation of the problem on the internet, rather than punishing the undesired behavior itself. At its worst, this focus on the platform rather than the actor promotes the dangerous idea that government should regulate generic technological capabilities rather than bad forms of behavior *per se*.

1. Intermediation in economics and law

The issue of the legal responsibility of intermediaries has a long history in economics and law (Lichtman & Posner, 2006), but its relevance to information and communication policy is not as well explored. Theories of freedom of expression are typically based on the simple paradigm of a speaker and a listener. The suppression of freedom of expression is conceived as interference with a speaker's right to express a viewpoint, or as interference with a listener's right to seek out and receive information.

Internet communications, however, connect speakers and listeners through a long chain of intermediary services. This includes

- the device and its operating system;
- local and backbone Internet access providers;
- domain name registrars, registries and nameservers;
- hosting services, content providers and content distribution networks;
- financial intermediaries; and
- web-based platforms such as search engines and social networking sites.

☆ This work had its origin in the 2011 Quello Lecture hosted by Michigan State University's Quello Center for Telecommunication Management and Law. The author wishes to express his appreciation to the Center and its Director, Professor Steven Wildman, for the opportunity.

E-mail addresses: miltonmueller@outlook.com, mueller.syr.edu@gmail.com

http://dx.doi.org/10.1016/j.telpol.2015.05.001

Please cite this article as: Mueller, M. L. Hyper-transparency and social control: Social media as magnets for regulation. *Telecommunications Policy* (2015), http://dx.doi.org/10.1016/j.telpol.2015.05.001

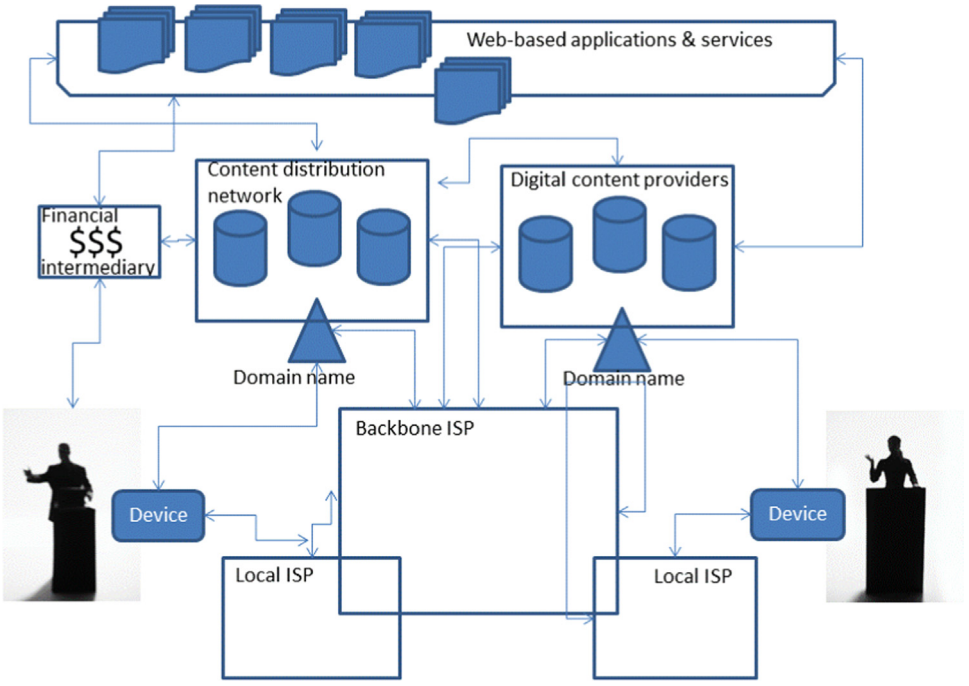

Fig. 1. Intermediation of speech on the Internet.

Though some are more concentrated than others, there are usually multiple suppliers in every segment of this chain, forming a complex, often market-driven system which it is now fashionable to call an "ecosystem" (Fig. 1).

The concept of freedom of expression needs to be attuned to this richly intermediated environment (Ardia, 2010; Goldman, 2004–2005). Specific speakers and listeners may not be directly accessible to authorities or litigants, or pursuing them individually may seem prohibitively costly. Thus, there is a temptation to seek out and leverage intermediaries that can affect the targeted communication. Kreimer (2006) provides an excellent legal and normative analysis of how intermediaries can be employed to disrupt or suppress expression indirectly. Noting that speakers and listeners can be affected through an intermediary, Kreimer formulated the idea of the "weakest link," the part of the chain of communication intermediaries that is most vulnerable to disruption. The disrupter could be a repressive government, a law enforcement agency or a clever lawyer acting on behalf of a private litigant. Finding the weak link reduces transaction costs; it may provider a closer target, a more visible, politically vulnerable target or a financially fatter target.

To some extent, policy makers in the US have understood the important relationship between freedom of expression and intermediary responsibility. A number of policy instruments in the early years of the Internet's development immunized intermediaries from liability for the actions of their users.[1] In the United States, the strongest form of protection came from Section 230 of the Communications Decency Act of 1996 (CDA) (1996). Section 230 immunizes interactive online services (OSPs) from specific types of legal liability stemming from content created by others. The protection includes news websites, blogs, email forums, and user-generated content sites such as Facebook and YouTube. It shields OSPs from defamation, privacy, negligence and other tort claims associated with publication (but not intellectual property claims).[2] It is important to note that Section 230 had two distinct goals, which may seem to be at odds with each other. It was intended *both* to immunize OSPs who did nothing to restrict or censor their users' communications, *and* to immunize OSPs who took some effort to discourage or restrict online pornography and other forms of undesirable content. Intermediaries who did nothing were immunized in order to promote freedom of expression and diversity online; intermediaries who were more active in managing user-generated content were immunized in order to enhance their ability to delete or otherwise monitor 'bad' content without being classified as publishers and thus losing their immunity from liability for the content they did not restrict.[3]

Normally, discussions of intermediary responsibility focus on the way the assignment of legal liability affects the incentives of the operators and the users posting information online, and whether the resulting incentive structure has good or bad effects on society or individual freedom (Perset, 2010). Those are important and valid aspects of the policy discourse.

[1] In addition to Section 230 of the CDA, discussed below, there was the Ecommerce Directive 2000 of the European Commission, and the Digital Millennium Copyright Act of 1998, which immunized various actions of Internet service providers from responsibility for the actions of their users.

[2] See "Section 230 of the Communications Decency Act," Citizens Media Law Center, http://www.citmedialaw.org/section-230.

[3] As the Court said in *Zeran v. America Online, Inc., 129 F.3d 327 (4th Cir. 1997)*, Sec. 230 was passed to "remove the disincentives to self-regulation created by the Stratton Oakmont decision." In *Stratton Oakmont, Inc. v. Prodigy Services Co.*, 1995 WL 323710 (N.Y. Sup. Ct. 1995), a bulletin board provider was held responsible for defamatory remarks by one of their customers because it did make efforts to edit some of the posted content.

Please cite this article as: Mueller, M. L. Hyper-transparency and social control: Social media as magnets for regulation. *Telecommunications Policy* (2015), http://dx.doi.org/10.1016/j.telpol.2015.05.001

But it tends to overlook some of the broader contextual and societal dynamics in play. To make those complex social forces visible, consider the following three incidents. In each case, hyper-transparency leads public discourse to attribute responsibility to the intermediary, regardless of their legal liability.

2. Three incidents

In August of 2011, there was rioting in London and other major cities in the UK. Some of the rioters used instant messaging tools and other forms of social media to coordinate their activities. In a desperate response, Prime Minister David Cameron raised the idea of blocking social media sites. The idea that something had to be done about instant messaging had bipartisan support. For a time, the UK was discussing the interception and disclosure of messages by authorities, the deletion of messages deemed to foment social unrest, the banning of suspected rioters from social networks, and even the complete shutdown of social networks during periods of unrest. More than one observer contrasted the British response to that of the Egyptian and Tunisian dictatorships where, only a few months before, the use of social media for political mobilization was hailed as a great thing; there was talk of "Facebook revolutions" and "Twitter Revolutions" and calls to extend social media everywhere (Khamis & Vaughn, 2011).

In May of 2006, a group of teenagers in Italy recorded themselves insulting and assaulting an autistic boy. The video was uploaded on Google by someone named Giulia Lisa in September of that year. The video received thousands of hits. There was a request by an organization advocating for the protection of people with Downs syndrome to take it down. Google, which receives thousands of such takedown requests every day, refused to do so until there was a court order, knowing that such requests are often abused to suppress legitimate expression. Eventually the proper authorizations were received and the video was taken down. Italian prosecutors nevertheless went after Google, arguing that the video violated the boy's privacy and should have been taken down more quickly. The Italian court convicted three Google executives of failure to comply with the Italian privacy code, and of criminal defamation (Sartor & de Azevedo Cunha, 2010). The Italian prosecutors claimed that "Google have a duty of care and responsibility; allowing videos to be shown where adults and children are being abused just states that it is acceptable behavior."

Craigslist is a classified ad service renowned for its easy and free posting, its simplicity and its early-internet ethic of noncommercial service. It contains a huge variety of forums for matching people with products and services of interest, as well as discussion boards on diverse topics. Among its categories are personal ads. Several years ago it created an 'erotic services' section because users of their personal ads asked them to get rid of the many solicitations from prostitutes that interlaced them. Later, at the request of State attorneys general, Craigslist began requiring a $10 fee paid by credit card and a working phone number to place an ad in that section. It also hired a lawyer to filter ads for suggestions of underage girls. But that was not enough. Craigslist was attacked repeatedly by politically ambitious state attorneys general and mass media news outlets for aiding and abetting illegal prostitution. And so under intense pressure, Craigslist removed the adult services category from its classifieds. Eventually it did so not just in the US, but also in other countries where prostitution is actually legal.

3. The fallacy of displaced control

In each of the cases described above, we see Internet intermediaries flagged for responsibility for the actions of their users, sometimes in an extreme, discriminatory way. Someone uses the Internet's communication capability for something unexpected. Authorities who do not like what happened demand the ability to track and monitor, block access to, or regulate the capability that was used. They operate under the assumption that if they had had that capability beforehand, they would have been able to prevent the bad things that happened. Or they demand that the intermediary who supplied the platform used take responsibility for eliminating the behavior.

It should be noted that in the United States the bare legalities of the cases did not determine the outcome. Whenever Craigslist went to court, for example, it was never found guilty of participating in or aiding prostitution, due in no small part to its Section 230 immunities.[4] Nevertheless, the response that the law immunized Craigslist from responsibility, and that there were good reasons to immunize them, sounded weak and evasive in the public discourse. Craigslist as intermediary was still perceived as the source of prostitution because it made it visible, and eventually was driven out of the business, even in countries such as Canada where the targeted activity is legal.

Similarly, authorities and others who like what social media platforms were involved in, such as Egypt's and Tunisia's use of social media to foster political mobilization, have proposed to subsidize or promote the capability. They operate under the assumption that putting that capability in the general population's hands will automatically produce a desired result—even when a few months later, politicians complain about the use of social media in riots.

[4] See for example Thomas Dart, Sheriff of Cook County v. Craigslist, Inc. 665 F. Supp. 2d 961 (N.D. Ill. Oct. 20, 2009). The Sheriff tried to hold Craigslist responsible for "facilitating prostitution," a criminal offense. The Court rejected that argument and upheld Craigslist's immunity. See also Voicenet Communications, Inc. v. Corbett, 2006 WL 2506318, at ⁎4 (E.D. Pa. Aug. 30, 2006), which directly addressed the question of whether section 230 preempts state criminal law and concluded that it does.

Please cite this article as: Mueller, M. L. Hyper-transparency and social control: Social media as magnets for regulation. *Telecommunications Policy* (2015), http://dx.doi.org/10.1016/j.telpol.2015.05.001

The cases all follow a similar logic:

- Social media applications were used to do X
- Ergo, regulating, shutting down or (if the result was considered positive) promoting the social media application puts society in control of X.

This is what I call "the fallacy of displaced control." Instead of punishing bad behavior, we strive to control the tool that was used by the bad actor(s). Instead of eliminating illegal materials or activities, we propose to eliminate internet access to illegal materials or activities. At its most extreme, this view leads to the conclusion that if a technological capability can be used to do bad things, then it is the capability itself that must be controlled, not individual behaviors or uses. The structure of the argument would in principle give authorities the power to monitor and pre-emptively block or control anything, because virtually anything can be used to do illegal things. An extreme example of this leap is the proposed *Protecting Children from Internet Pornographers Act of 2011*. It required ISPs to keep track of every website that users visit for at least a year and make them available to the federal government without a warrant. The law was really a broad data retention act that targeted every user indiscriminately, regardless of whether there is any plausible suspicion of illegal child porn. The assumption underlying it is that we all might be child abusers and the data about our activity might be useful in catching us and therefore law enforcement agencies should secure access to it.

The combustible combination of hyper-transparency and displaced control raises numerous questions. In the Google case, why were the punishment and prosecution so focused on the video publishing platform and not on the culprits who actually abused the boy and posted the video? Most of the social blame associated with the incident was assigned to Google. The student bullies got off with some community service. The person who posted the video was neither charged with anything nor even called to testify about the privacy terms offered by Google when she posted the video.

In the Craigslist case, if local law enforcement wanted to arrest or stop people engaged in prostitution, why would not they welcome the fact that easily accessible Internet classified ads openly display offers from sellers? The ads provided a basic location, a phone number and email address, a description and even pictures of the suppliers of the illicit service. Law enforcement would have most of the information it needs to find illicit traders and save girls from "trafficking." Would shuttering these advertisements reduce prostitution and trafficking, or simply remove it from view?

4. Classified ads and prostitution

To answer these questions, we need to explore the dynamics of public discourse. This will show more directly how hyper-transparency makes social media a kind of magnet for social control efforts. The details and process of the Craigslist case exemplify the point I am making especially clearly. Its services proved to be easy targets for "ambush journalism," in which the Internet service provider's unwitting facilitation of activity deemed socially undesirable allowed them to be shamed before a mass public and held responsible for the activity in question.[5]

Indeed, the entire incident was literally replicated a year or two later. After Craigslist shut down its erotic services section, the same type of advertisements shifted to a web-based classified ad service known as Backpage.com, something of a Craigslist copycat. Soon Backpage became the target of the same kinds of pressures and commentary that Craigslist had gone through. Cable television news channel CNN, for example, highlighted the fact that the online services were used to match sex workers with willing customers. But CNN, like many others involved, seemed to think that prostitution itself (though illegal in the US) was not a gaudy enough target. It shifted the debate away from prostitution per se to trafficking in underage girls. CNN chose to shine its media spotlight not on the adult sex workers who were placing classified ads, but on pimps who were exploiting underage girls. The dialogue about Backpage and Craiglist thus became a dialogue about human trafficking in minors. CNN went so far as to claim that "the internet has greatly expanded child prostitution and child sex trafficking. In particular, witnesses cited online advertising sites such as Craigslist and backpage.com as facilitating the ability of people to hire child prostitutes."

In neither case were the critics of the classified ads able to produce any Craigslist or Backpage ads that openly advertised sex workers under the legal age. Indeed, when confronted with the argument that it was actually better for sex workers to have the ads more open and transparent so that they could be tracked and monitored, CNN's Anderson Cooper did not directly engage with this argument. Instead, he shifted the discussion to an interview with "some of the mothers of teen victims." The program then went into the story of a 15 year old girl who ran away from home and ended up with a man who is alleged to have beat and raped her and then placed ads for her on Backpage. We heard from one other mother with a similar story. Her 14 year old ran away from home and "was later prostituted by a man she met at a bus stop," who was alleged to have advertised her on Backpage.com.

New York Times reporter Nicholas Kristof took the dialogue further downhill, targeting the advertising platform with a video headlined: "Age 16, She Was Sold on Backpage.com." But fact-checking revealed that Kristof had fabricated his basic story line. According to court testimony, the girl he was writing about was 16 in 2003. At that time, *Backpage.com did not*

[5] Tony Ortega, "CNN's Amber Lyon Ambushed Craigslist. CNN leads the media's mass paranoia over a nonexistent epidemic" *Village Voice,* July 6 2011 http://www.villagevoice.com/2011-07-06/news/stuck-in-trafficking/.

Please cite this article as: Mueller, M. L. Hyper-transparency and social control: Social media as magnets for regulation. *Telecommunications Policy* (2015), http://dx.doi.org/10.1016/j.telpol.2015.05.001

exist as a business, so she could not have been sold on it. FBI Records indicated that pimps had indeed been brokering the services of the underage victim in the summer of 2005 in Boston, New York and Philadelphia. But Backpage did not exist in any of those cities at that date, either. In reality, the girl had been working corners, bars and hotels in the old-fashioned, less transparent methods of prostitution. But the link between Backpage and child abuse was so tempting it had to be invented if it was not true. It was Backpage, after all, which made prostitution visible to the public. Kristof and various state Attorneys General kept suggesting that online classified ads were fundamentally responsible for the existence of the problem of underage sex work and human trafficking. Implicitly – for an explicit statement of the proposition would be less than credible – they conveyed the message that if Backpage was shut down, 14 and 15 year old runaways would no longer fall into the hands of abusers.

One rather obvious test of CNN's thesis is whether the rise of internet-based classified advertising is correlated with increases in the number of underage prostitution arrests. If the classified ads had a causal effect of increasing both the demand and the supply of underage sex workers, the rise of these social media services from the middle of the decade to 2009 should have produced a significant change in the arrest statistics. Yet it has not. On the contrary, according to statistics from the 37 largest cities in the U.S. compiled by a *Village Voice* reporter, the number of arrests of underage suspects for prostitution dropped nationwide from 2000 to 2009 (Cizmar, Conklin, & Hinman, 2011). While a few major cities saw an increase in arrests (notably Dallas and Los Angeles), most cities, including New York, Boston, Philadelphia, Chicago and Miami, saw significant declines over that decade. Across all 37 cities the average number of annual arrests decreased by 20% from the 2000-2002 period to the 2006–2009 period. So it is clear that visibility on the Internet is not worsening the situation, and is actually correlated with an improvement. Yet none of the media outlets covering this issue bothered to check any statistics, with the exception of the *Village Voice*, which as the owner of the beleaguered Backpage.com had a strong incentive to do so (Cizmar, et al., 2011).

This willful avoidance of facts that might interfere with the narrative extends to another problem often attributed to the Internet – the increase in child abuse images, also known as child pornography, which is also frequently linked to the rise of the Internet. As child protection advocates confronted the Internet and pushed for content regulation from the late 1990s on, they frequently spoke of pedophilia as an "epidemic" that was transmitted through the Internet.

Child pornography is wrong morally because it involves children who are too young to provide proper consent or to resist manipulation and abuse. But if one checks factual material about sexually oriented child abuse, one discovers a rather startling fact:

> The past two decades have witnessed some rather remarkable declines in the number of child physical and sexual abuse cases… entering child welfare in the United States. Declines on the order of 50% or more have been found. These declines have been observed across child welfare data, law enforcement data and in population based surveys (Chaffin & Jones, 2011).

The authors of that quote face up to an equally sobering fact about the reception accorded these facts:

> The ostensibly good news has sometimes been met with mixed reactions from practitioners and advocates, who may see a disconnect between the data and their daily work experiences, or who may be concerned that declining abuse rates could lead to corresponding declines in funding or momentum for addressing child maltreatment. Child abuse advocacy has for decades been premised on a collective narrative that the problem is at crisis levels and getting worse.[6]

The idea of an Internet-driven epidemic of child porn may be nothing more than a byproduct of our enhanced ability to track it or encounter it, which is itself due to the Internet. Insofar as child abuse materials are traded or distributed on the Internet, they become far more visible and track-able than they would be otherwise, and the public discourse about it actually places more normative pressures on child abusers than existed before.

Thus, in both classified prostitution ads and Internet-based child pornography, hyper-transparency and displaced control seem to have produced major effects on public discourse and public policy. Our improved ability to see social activity objectified and recorded online leads to the (often incorrect) conclusion that certain problems we can see there are rapidly growing; it also provides support to those whose professional interests or personal ideology make them want to prioritize the problem.[7] Politically ambitious prosecutors, from the US to the UK to Italy, eagerly exploit such perceptions to propose or impose legal and regulatory restraints on Internet intermediaries. This process is very robust, and occurs even when the narrative is unsupported by – or directly contradicted by – statistical data.

[6] See also *Child Maltreatment 2009*, a statistical compilation published by the US Health and Human Services Department: http://www.acf.hhs.gov/programs/cb/pubs/cm09/cm09.pdf.

[7] One former sex worker and blogger compares what she calls the "trafficking hysteria" to the satanic cult scare of the 1980s, which culminated in the McMartin Preschool trial. "Both revolve around gigantic international conspiracies which supposedly abduct children into a netherworld of sexual abuse; both are conflated with adult sex work, especially prostitution and porn; both make fantastic claims of vast numbers which are not remotely substantiated by anything like actual figures from law enforcement agencies or any other investigative body; both rely on circular logic, claiming the lack of evidence as "proof" of the size of the conspiracy and the lengths to which its participants will go to "hide" their nefarious doings; both encourage paranoia and foment distrust of strangers, especially male strangers; etc, etc, etc." Maggie McNeill, *The Honest Courtesan*, May 20, 2012 http://maggiemcneill.wordpress.com/2012/05/20/traffic-jam/.

Please cite this article as: Mueller, M. L. Hyper-transparency and social control: Social media as magnets for regulation. *Telecommunications Policy* (2015), http://dx.doi.org/10.1016/j.telpol.2015.05.001

5. The duality of intermediary responsibility

There are two prongs to the problem here. One is that the displacement of societal control can threaten the legal immunities that have contributed to the blossoming of Internet-based communications, including especially user-generated content sites. The other is that it can push intermediaries into overly aggressive, unaccountable self-policing, leading to arbitrary and unnecessary restrictions on online behavior.

The challenges of Internet governance have revived pressures to look to intermediaries for control. Social media platforms are visible and prominent, and easier targets due to the problems of cross-jurisdictional enforcement and the problems of attribution. This has led to a growing number of political and operational challenges to the immunities of internet intermediaries, and to a growing effort to delegate regulatory efforts to them. Rather than being seen as a pillar of online freedom of expression, the classic immunities are now seen by many as either a "shield for scoundrels" (Ardia, 2010) or as some kind of infant industry protection that is no longer needed because the Internet is not new or special any more. The push for intermediary responsibility comes on four fronts: copyright protection, which seeks to make Internet access providers police users for illegal file sharing (Bridy, 2010; Horten, 2011; Mueller, Kuehn, & Santoso, 2012) or domain name registrars and registries responsible for illegal sites; cyber-security, which seeks to make ISPs more responsible for thwarting botnets and other security threats (van, Eeten, Bauer, Asghari, Tabatabaie, & Rand, 2010); content regulators, who want social media platforms and ISPs to block access to certain kinds of materials (Bambauer, 2009; Stol, Kaspersen, Kerstensa, Leukfeldta, & Lodder, 2009); and from law enforcement agencies who want a strengthened and generalized surveillance and identification capability to be built into intermediaries' systems.

The policy debate here is complicated by the fact that Internet intermediaries can and do take regulative responsibilities on their own, and this is often a good thing. OSPs can internalize some of the negative externalities of the Internet. In some cases operators may be bowing to irrational social pressures, but they may also be engaged in a legitimate attempt to enhance the value of their brand name and improve the quality of their service by discouraging forms of behavior that make their platforms unattractive or harmful to their users (Marlin-Bennett & Thornton, 2012). Facebook, e.g., has imposed restrictions on racist speech on its platform. Many Internet freedom activists want Internet platforms that make up a major part of the online public sphere to avoid regulating and restricting speech, while at the same time asking them to exercise certain forms of social responsibility (MacKinnon, 2012).

Moreover, new technological capabilities make it possible for larger, well-capitalized intermediaries to define automated algorithms that scale up their control of mass interaction platforms. Google, to use just one example, has developed its ContentID technology, which allows copyright owners to register their works and be alerted any time someone uploads a sound or video file that matches the fingerprint of their copyrighted work. Even the businesses resisting intermediary responsibility can be subtly (and sometimes not-so-subtly) undermining it.

6. Conclusion

The power of the Internet has contributed to the idea that we can control society and preempt or prevent anything – from riots to copyright violations – through surveillance and manipulation of communications intermediaries. In the past we spoke of the Internet as a free place. It seems that now, the Internet is the *first* place we look to control behavior. Why? There are many causes, but this paper focuses on one: the extreme transparency fostered by social media.

Internet applications make social and technical processes hyper-transparent. Human activities, in all their glory, gore and squalor, take place in open, publicly visible mass-interaction platforms provided by commercial third parties. These platforms generate storable, searchable records and their users leave attributable, recordable tracks everywhere. The objectification of social interaction in the cyber environment, and the ease with which we can rummage through the objectified remains, makes it a magnet for social control efforts. It often lends itself to a displacement of social control efforts by inadvertently supporting the idea that human activity itself can be engineered and controlled by meddling with communication processes. When we see problems displayed in the online environment, or online tools are used to facilitate real-world crimes, we tend to link the two, and jump to the conclusion that what we see online can be programmed and controlled through online means. What often happens, however, is the fallacy of displaced control. Instead of controlling the behavior, we strive to control the intermediary that was used by the bad actor. Instead of eliminating the crime, we propose to eliminate internet access to the crime. It is as if we assume that life is a screen and if we remove unwanted things from our screens by controlling internet intermediaries, we have made life better and solved life's problems.

To some extent, no doubt, this is a temporary effect caused by the newness of the new media. Left unchecked, however, this could become a dangerous trend. There is in principle no aspect of human behavior on the Internet that you cannot see, restrict access to, or subject to algorithmic regulation. So we need to rethink what freedom of expression means and how the rights of private intermediaries interact with the rights of individuals, state power and the legitimate needs of law enforcement.

References

Ardia, David (2010). Free speech savior or shield for scoundrels: an empirical study of intermediary immunnity under Section 230 of the Communications Decency Act. *Loyola of Los Angeles Law Review*, *43*(Winter), 373.

Please cite this article as: Mueller, M. L. Hyper-transparency and social control: Social media as magnets for regulation. *Telecommunications Policy* (2015), http://dx.doi.org/10.1016/j.telpol.2015.05.001

Bambauer, Derek E. (2009). Cybersieves. *SSRN eLibrary(Journal Article)*
Bridy, Annemarie. (2010). Graduated response and the turn to private ordering in online copyright enforcement. *Oregon Law Review*, *89*, 89–132.
Chaffin, Mark, & Jones, Lisa (2011). Declining rates of child sexual abuse and what this really means. *Webinar*
Cizmar, Martin, Conklin, Ellis, & Hinman, Kristen. (2011). Real men get their facts straight: Ashton and Demi and sex trafficking. *Village Voice*, June 29.
Communications Decency Act of 1996 (CDA). (1996) (pp. Section 230).
Goldman, Eric. (2004–2005). Speech showdowns at the virtual corral. *Santa Clara Computer & High Technology Law Journal*, *21*, 845–870.
Horten, Monica M. (2011). *The copyright enforcement enigma: Internet politics and the 'telecoms package'*. London: Palgrave-MacMillan.
Khamis, Sahar, & Vaughn, Katherine. (2011). Cyberactivism in the Egyptian revolution: How civic engagement and citizen journalism tilted the balance. *Arab Media and Society*, *13*(Summer).
Kreimer, Seth (2006). Censorship by proxy: The first amendment, Internet intermediaries, and the problem of the weakest link. *University of Pennsylvania Law Review*, *155*(1), 11–101.
Lichtman, Douglas Gary, & Posner, Eric A. (2006). Holding Internet service providers accountable. In F. Mark, Grady, & Francesco Parisi (Eds.), *The Law and Economics of Cybersecurity*. Cambridge: Cambridge University Press.
MacKinnon, Rebecca (2012). *The consent of the networked: The worldwide struggle for Internet freedom*. New York: Basic Books.
Marlin-Bennett, Renee, & Thornton, E. N. (2012). Governance within social media websites: Ruling new frontiers. *Telecommunications Policy*, *36*(6), 493 -.
Mueller, Milton L., Kuehn, Andreas, & Santoso, Stephanie M. (2012). Policing the network: Using DPI for copyright enforcement. *Surveillance and Society*, *9*(4).
Perset, Karen (2010). *The economic and social role of Internet intermediaries*, Vol. 1. Paris: OECD49.
Sartor, Giovanni, & de Azevedo Cunha, Mario Viola (2010). The Italian Google case: Privacy, freedom of speech and responsibility of providers for user-generated contents. *International Journal of Law and Information Technology*, *18*(4), 356–378.
Stol, W. Ph., Kaspersen, H. K. W., Kerstensa, J., Leukfeldta, E. R., & Lodder, A. R. (2009). Governmental filtering of websites: The Dutch case. *Computer Law and Security Review*, *25*, 251–262.
van Eeten, Michel, Bauer, Johannes M, Asghari, Hadi, Tabatabaie, Shirin, & Rand, Dave. (2010). *The role of Internet service providers in botnet mitigation: An empirical analysis based on spam data.* In Paper presented at the Workshop on the Economics of Information Security. Cambridge, MA.

Please cite this article as: Mueller, M. L. Hyper-transparency and social control: Social media as magnets for regulation. *Telecommunications Policy* (2015), http://dx.doi.org/10.1016/j.telpol.2015.05.001