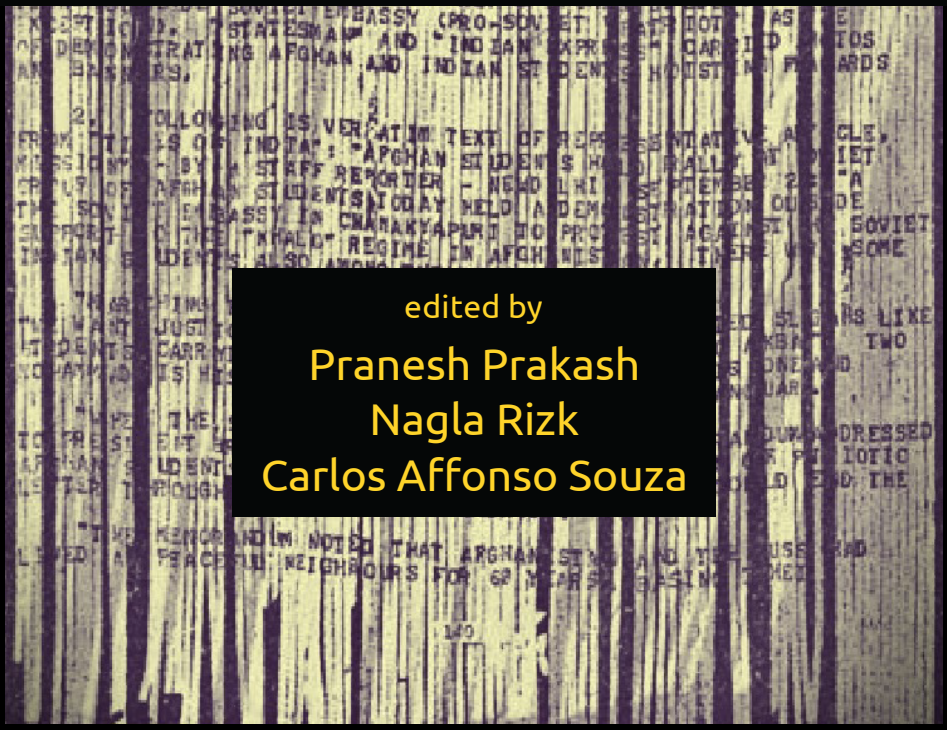
ACCESS TO KNOWLEDGE RESEARCH

GLOBAL CENSORSHIP

Shifting Modes, Persisting Paradigms



edited by

Pranesh Prakash

Nagla Rizk

Carlos Affonso Souza

GLOBAL CENSORSHIP

Shifting Modes, Persisting Paradigms

edited by

Pranesh Prakash
Nagla Rizk
Carlos Affonso Souza

ACCESS TO KNOWLEDGE RESEARCH SERIES

Front cover image: "Documents seized from the U.S. Embassy in Tehran", a public domain work created by employees of the Central Intelligence Agency / embassy of the United States of America in Tehran, depicting a shredded document that was seized by Iranian students in 1979, available online on the Wikimedia Commons at <https://commons.wikimedia.org/wiki/File%3AEspionage_den02_72.png>.

Global censorship: Shifting modes, persistent paradigms /

edited by Pranesh Prakash, Nagla Rizk & Carlos Affonso Souza.

isbn 978-1-329-33274-4 (U.S.A. paperback edition)

isbn [] (India paperback edition)

isbn [] (open access online edition)

I. Pranesh Prakash

II. Nagla Rizk

III. Carlos Affonso Souza

Set in Sorts Mill Goudy (Open Font Licence) and Ubuntu (Ubuntu Font Licence).

Typesetting and book production by Pranesh Prakash.

20150127

TABLE OF CONTENTS

ACKNOWLEDGEMENTS

The editors would like to thank the organizers of the Global Censorship conference at Yale in 2012, where many of the chapters contained here were first presented. We would like to thank profusely all the authors — who not only generously contributed their scholarship and research, but also served as peer commenters, and without a single protest agreed to release this book under an open copyright licence.

In addition, there are a number of people who have helped us greatly, who deserve especial thanks. From Yale, the Information Society Project's Jack Balkin helped provide the impetus for this book, while Margot Kaminski and Valerie Belair-Gagnon ensured that this book, much tarried at times, finally came through. Natasha Mendez and Heather Branch were fantastic, as always, in providing much-needed logistical support. From Cairo, Lina Attalah was indispensable, joining in as a peer commenter, while Sylvia Zaky ensured we stuck to our deadlines, and Stefanie Felsberger was most helpful, contributing both to editing as well as the logistics. Nevin Elwan's design skills helped nudge us toward a final decision on the cover for this book.

We also extend our deepest gratitude to Richard Bartlett, without whose generous support this book would not have been possible.

PREFACE

Nagla Rizk, Carlos Affonso Souza & Pranesh Prakash

This book has its origins in a network — the Access to Knowledge Global Academy — and a meeting — the Global Censorship Conference in 2012.

THE NETWORK

Organized around a series of 'Access to Knowledge' conferences, promoted by Yale Law School's Information Society Project (ISP) since 2006, the Access to Knowledge Global Academy (A2KGA) was created as an informal network of scholars and researchers dedicated to building capacity for research, education, and policy analysis promoting access to knowledge.

Representing a rich geographical diversity, the members of A2KGA include institutions from Brazil, China, Egypt, India, South Africa and the United States. The network was formally launched during the third A2K conference, held in Geneva in September 2008, coinciding with a meeting of the World Intellectual Property Organization's (WIPO) Standing Committee of Copyright and Related Rights.

In August 2009 the network organized a gathering at Yale Law School bringing together the different members of the Academy. In November of that year, the same group held a public workshop titled "Research on Access to Knowledge and Development" at the United Nations-convened Internet Governance Forum, in Sharm El Sheikh, Egypt.

In January 2011 a gathering was convened at the University of Cape Town in South Africa. In August of that year, a workshop showcasing current research developed by members of the network was organized at the sidelines of the first Global Congress on Intellectual Property and the Public Interest, held at American University's Washington Law College. The group also organized a workshop to present research that led to this book

during the second Global Congress on Intellectual Property and the Public Interest, held in Rio de Janeiro in 2012.

In addition to the public gatherings and seminars, the most tangible output from the network has been the launch of a series of books on Access to Knowledge. With support from the MacArthur Foundation, and partnering with Bloomsbury Academic, three volumes of the Access to Knowledge series have been launched, focusing on debates arising from Brazil, Egypt and India respectively. While each of these books is available for sale in hard copy, they are openly licensed under a permissive Creative Commons licence, and are freely available for digital download as well. One volume, Access to Knowledge in Egypt, was also published in paperback, and available for sale at a modest price in the Middle East.

The goals of the A2KGA are to promote access to knowledge as a framework for policy-making, to advance collaborative research that both responds to immediate needs and at the same time develops a long term positive vision, as well as to develop model curricula to educate students and policymakers in new ways of thinking about knowledge policy.

To do this, the A2KGA partners draw on disciplinary strengths in law, economics, political science, engineering, and beyond, working to build communities of A2K researchers both locally and globally and develop a new generation of global scholars prepared to grapple with the hard questions facing the A2K agenda over the next decades.

THE CONFERENCE

Access to knowledge stands against intellectual enclosures. A more comprehensive and robust understanding of A2K, therefore, calls for a more and newer intricate understanding of censorship and its problematics.

Censorship often reinforces existing power imbalances that serve narrow elites at the expense of democratic participation. It has many faces and many tools, being political, economic, technological and even psychological. In practice, knowledge ends up being excludable through the erection of barriers of any or all of these different forms. Such barriers have inseparable socio-economic and political repercussions. Ultimately, censorship is detrimental to human development and to human rights.

The idea to gather efforts around the A2KGA network to work on censorship issues and publish a case-oriented book containing a series of case studies came along during the Global Censorship Conference, organized by Yale's Information Society Project in March, 2012. The event brought together a number of participants of the network to present on censorship issues in their respective country or region. The network expanded then its initial focus on how access to knowledge challenges established notions of intellectual property to encompass the framing of A2K concerns in connection to the enjoyment of freedom of expression and related rights.

The Global Censorship Conference explored the technical, legal and political perspectives on the issue of censorship and how new technologies are being applied to either enforce restrictions over discourse or to circumvent the very same measures. Technology can be a tool that fosters speech at the same time that it can be an instrument of censorship and surveillance. Its role in a networked world cannot be underplayed and to debate how government, companies, civil society and individuals resort to technology to communicate or ultimately to restrict or deny access to information is paramount for the better understanding of this ever- changing reality.

This perspective was also presented at the 2013 and 2014 annual workshops held by the Access to Knowledge for Development Centre (A2K4D) at the American University in Cairo. A number of case studies that are featured in this book were presented at the workshops, fostering debate around the connection between censorship practices and A2K concerns.

FROM A2K TO CENSORSHIP

Access to Knowledge (A2K) refers to the right to receive and to participate in the creation, modification and extension of information, tools, inventions, literature, scholarship, art, popular media and other expressions of human inquiry and understanding. Within the A2K paradigm, knowledge is comprehensively conceptualized to extend beyond information and data, being embedded in the theoretical grounding of the economics of knowledge and human development.

Knowledge has unique characteristics. For example, knowledge acts both as an input and output of its production process. In order to produce

a research paper, one commences by reviewing the literature and researching other material written on the topic. Wider access to knowledge, therefore, facilitates the smooth and thorough creation of new knowledge. Any blockage impacts not only the stock, but also the flow of new knowledge production. In the short run, monopoly over the creation of knowledge creates a static inefficiency.

Most notably, knowledge has public good characteristics. Unlike a private good, knowledge is non-rival, meaning that one person's consumption does not take away from another's. If two, or indeed two thousand, people learn a theory, they have not used it up, or "spoilt" it, for each other. One may actually argue that the value of knowledge increases with the increase in the number of its users. Indeed, the body of code written to produce open source software has only gotten richer because of its opening up to a large community of collaborating developers and programmers.

Strict economic analysis stipulates that pricing should be set according to the marginal cost. But the marginal cost of an extra user of a public good – knowledge in this case – is zero. Economic efficiency, therefore, would set the optimal price of knowledge at zero, meaning free access to all. But this brings up the issue of incentives: who wants to produce a good whose price is zero? The market therefore fails when knowledge is treated as a private good. From an efficiency point of view, it is optimal for knowledge to be provided to all via free access. On the other hand, there is no incentive for anyone to produce free knowledge. This tension is commonly known as the "access vs. incentives trade-off".

The A2K paradigm offers a nuanced analysis towards the resolution of this tension. It works towards finding alternatives that help achieve a balance between access and incentives. On the access side, knowledge output can now be provided in different versions especially given today's technologies. For example, a book can be provided for sale of the hard copy, with free content available online. Free access of one version does not preclude the possibility of parallel versions offered for pay.

In addition to versioning, financial remuneration can be indirectly achieved through novel business models that provide financial returns on differentiated value added. For example, businesses built around open source software offer a price for customization services while freely shar-

ing their code. Musicians can be remunerated for their live concerts while offering their music freely online. Within such "freemium" offering, additional options can be provided, e.g. optional payments for online albums. Media content can be made freely available online, but subscription fees can be collected for an additional mobile application service that repackages content. The vast development in digital technologies facilitates options for devising and implementing such models.

But the issue extends beyond market efficiency and equity and further connects to core aspects of human development. At the heart of the A2K paradigm is the role of knowledge to promote the right to health, education, housing and other aspects of a dignified human life. As such, the paradigm is not limited to the institution of economic models that balance access and incentives, but also consists of demands that span a wide range from limitations and exceptions on copyrights to regulation of anti-competitive practices and elements of Internet freedom to compulsory licensing provisions for a wide range of knowledge goods."

Liberty and openness are core values of the A2K paradigm, where knowledge goods and tools are democratized for the benefit of all. Individuals' and society's rights to participate in the creation of knowledge and its dissemination extend beyond those of just consumption. The Universal Declaration of Human Rights states, "[e]veryone has the right freely to participate in the cultural life of the community, to enjoy the arts and to share in scientific advancement and its benefits" (UDHR, Article 27). And so, beyond calling for the removal of inefficient economic barriers, the access to knowledge paradigm is a political demand for openness and democratic participation.

The A2K paradigm calls not only for the 'openness' of content, but also of the tools that enable participation in the creation of such content. Such tools enable individuals to exercise their right to freedom of expression and democratic participation. Utilizing digital tools to hold governments accountable; to increase the reach of information, and access to diverse views through citizen journalism; to expose regimes' shortcomings; to engage in participatory budgeting and planning; and to customize innovations to suit developing countries are some of the possibilities that are more readily available once tools are accessible. However, digital tools are

not one-sided: they equally enable regimes access to greater surveillance of citizens, enable more efficient targeting of dissenting voices, and allow greater controls over information.

The call for such access is a cornerstone of the A2K movement and implicates policymaking across the spectrum, from education to Internet governance to research and development. Accordingly, the A2K movement is positioned at the intersection of political and economic decision-making processes and is a manifestation of their inseparability, as civil and political rights are inextricably linked with economic and social rights.

The A2K framework seeks to ensure that the potential for knowledge-based development and growth is maximized through programmes, technologies, and business models that enable knowledge to be shared widely. In this way, knowledge resources can be leveraged for the benefit of all, rather than be constrained or monopolized for the benefit of a few.

The present book aims to provide future studies on the interface between access to knowledge and censorship with a series of cases and in-depth reflections over this connection. As Jack Balkin pointed out during his presentation at the Global Censorship conference, a system of free speech depends not only on the mere absence of censorship, but also on an infrastructure of free expression.

In this sense, as we delve deeper on the cases and reflections provided in this book, the elements and principles of this infrastructure slowly come to light. As you read this book, keep in mind that we do not seek in this book to provide a comprehensive analysis of the features of this technical, legal and political infrastructure that fosters speech and knowledge. However, the cases reported and discussed herein provide an introduction to the researcher who wants to better understand the scenario of a specific country or censorship practice. At the same time, we hope that the narrative and the analysis of the cases can work as an invitation to the reader to expand her knowledge of the interface between censorship and technology.

INTRODUCTORY FRAMEWORK

Margot Kaminski & Pranesh Prakash

In 2006, during the Access to Knowledge conference organized by the Yale Information Society Project, Jack Balkin gave a speech in which he identified three broad points about the theory of access to knowledge:

- First, Access to Knowledge is a demand of justice.
- Second, Access to Knowledge is both an issue of economic development and an issue of individual participation and human liberty.
- Third, Access to Knowledge is about intellectual property, but it is also about far more than that.[1]

In his 2007 address at the second Access to Knowledge conference, Balkin provided some ideas about what that "far more than that" consisted of. He situated access to knowledge as the goal of a broader 'knowldege and information policy', of which freedom of speech is a part. Freedom of speech and access to knowledge depend on what Balkin identifies as an 'infrastructure of free expression',[2] which enable 'democratic access to and participation in cultures'.

This book seeks to address that larger view of access to knowledge by bringing together a series of case studies that provide a broader picture of what censorship is today. One of the most difficult problems faced by individuals working in this area is definitional.[3] Given the broad range of speech-related tactics that different countries use, what do we mean when we use the word "censorship?"

At the Global Censorship conference held at Yale Law School in March 2010, which laid the foundation for this book, Balkin, once again, presented a useful framework for beginning to answer this question.[4] Censorship — which Balkin calls 'speech regulation', to avoid the pejorative connotations that word carries — can be divided into two rough types: "old school" and "new school". Old-school censorship has characteristics of direct and salient use by the state of its power to detain, block, or destroy. For instance, the police could show up at a journalist's home, confiscate all written materials, and throw the journalist in jail. This is the type of censorship that is instantly recognizable as censorship. Likewise, using a state agent to black out objectionable passages in all copies of a book, or to use the court system to prevent distribution of the book altogether, is old-school censorship. Even when the state co-opts private parties — as happened during the McCarthy witch-hunts against communists in the United States — the censorship that takes place is still quite visible, and easily identifiable as censorship.

New-school censorship is markedly different in several ways. It is often not performed by the state itself, but is either outsourced through third-parties — such as internet service providers, web services, or financial intermediaries — or is performed by private actors without the active direction or involvement of the state. It is often indirect, and communication is blocked through less obvious means. It also tends to rely on digital surveillance, and in many cases on state access to infrastructure and authority over digital infrastructure providers.

Old-school censorship is a dying breed in many democracies where freedom of expression is guaranteed by a constitution or a bill of rights. New-school censorship, on the other hand, occurs regularly, but is often not readily identified as 'censorship' — hence, the definitional problem. In more repressive regimes, new school censorship interacts with the old in deeply problematic ways. A state may pursue both forms of censorship at the same time: outsource certain kinds of censorship to private parties, and still arrest journalists on false charges and throw them in jail. The two types of censorship also share common features; surveillance has played a role in both types, and it is arguably more ubiquitous today than ever before.

Despite these notable differences, this book does not claim that there is a bright-line division between old- and new-school censorship, nor between digital and non-digital censorship, nor does it claim that all experiences of censorship are equivalent in harm or scope. Rather, it seeks to illustrate the range of tactics used by states — and corporations — today and recently, that control and restrict the present knowledge environment, and the infrastructure of free expression, both online and offline, and through them to illuminate some of the changes we are seeing in the nature of censorship itself.

The chapters of this book address a wide variety of censorship activities taking place around the world, across nine countries in four continents. Some of the country chapters focus exclusively on digital case studies, while others look at both digital and offline censorship as inseparable. In these chapters, two important questions are repeatedly addressed, implicitly or explicitly. First, what is meant by censorship, and what shapes and forms does it take in actual practice? Second, how do organs of the state and civil society engage with the practice and contours of that censorship, and create possibilities for accountability and for change?

DEFINING CENSORSHIP

The first question of "what is meant by censorship" can be answered along three observable axes: the justifications provided, the actors involved, and the methods used. Censors regularly offer justifications for censorship, ranging from preventing criticisms of the government, to protecting national security, to balancing speech against other rights such as privacy, or intellectual property, or personal dignity. Each case in this book addresses one or more of the justifications states give for creating censorship regimes. Some of these directly target expression, while for others restrictions on free expression is a collateral cost. Sometimes a technical regime that is built with one justification in mind — say, curbing online distribution of child pornography — may end up serving another — enforcement of maximalist interpretations of copyright law.

In identifying what is meant by censorship in each case study, the authors have paid close attention to which actors are involved. States increasingly do not regulate speech directly. They employ intermediaries,

encourage private contracting, or permit private censorship. Censorship can involve multiple actors in different capacities. An actor-oriented categorization of censorship could divide it up as: direct state censorship, state-directed censorship, state-enabled censorship, state-independent private censorship, societal censorship, and self-censorship. In each of these categories — with the exception of societal and self-censorship — the act of censorship can be seen as being lawful, unlawful, or even extra-legal. Most laws protect against state censorship, but in mature democracies like the United States of America or India there is little naked state censorship, with state-directed, state-enabled, state-independent private, societal and self-censorship being the more important conceptual categories.

States also employ vastly different methods for censoring. Some go after communications infrastructure by employing broad 'kill switches', as in Egypt. Others engage in surveillance, thereby on occasion chilling the speech of journalists or activists or minorities, as in the USA and Myanmar. Some establish liability regimes, whether criminal or civil, directed at users or communication intermediaries, as in South Africa, India, and China. Others revise right to information laws to prevent journalists from accessing government information. Some continue to perpetuate old school censorship by employing the enforcement powers of the state, as has been done in Brazil through the judiciary. Each case study in this book addresses one or more censorship method chosen by the state, or in some cases private entities, to stop or shape some kind of speech, or that is chosen for other reasons, but structurally achieves the result of interfering with free expression. Importantly, by using the word 'censorship' we do not necessarily impute malicious motivations to the actor that is censoring. In some cases, it is a lack of understanding of the implications of their actions that leads to censorship, as we see in some of the case studies, for example, from South Africa and India.

OVERVIEW OF CHAPTERS

While there is no way of succinctly capturing all the different ideas contained in the various chapters of this book, we will briefly walk through the themes that they touch upon. Dr. Laura DeNardis's chapter titled "The Privatization of Free Expression", kicks off the book, and in it

she explores the role of Internet governance, especially its technical governance and what she terms "private public policy", in determining whether the "technical characteristics providing infrastructures of free expression" are preserved and promoted on the Internet.

In her chapter on the United States of America, Anjali Dalal looks at the evolution of the chilling effects doctrine in American free speech law, and some of the adverse consequences of domestic mass surveillance, especially on minority populations. In the second chapter to look at the USA, Prof. Christina Mulligan writes of the use of copyright law to remove non-copyright-infringing material, including political speech and cultural speech, through intermediary liability-linked content removal requests, and through "seizures" of domain names: a step unprecedented in other countries. She notes how our inherent sense that censorship ostensibly for copyright reasons bring forth lesser vigilance: "the public would likely have been up in arms", she notes, if in the scenario she describes, "a magazine printing press" had been seized "instead of a domain name".

In their joint chapter on Zimbabwe and South Africa, Prof. Caroline Ncube and Dr. Eve Gray paint a broad-brush overview of the law relating to access to information, official secrets, intermediary liability, and insult of the state by going through a wide assortment of instances of censorship. They examine different kinds of instances of censorship, ranging from direct ("old-school") state censorship through arrest of journalists to self-censorship due to the atmosphere created by a political party.

Expanding on one of the threads that Dr. Gray touches upon in that chapter, Andrew Rens presents detailed analysis of the intermediary liability regime and its constitutionality. By doing so, he answers the question of whether "interdiction of the means of speech be characterized as censorship, when it is carried out by one non-state actor at the behest of another?"

In a markedly different take on the theme, the chapter by Rebecca Wexler and Carey Murphey looks not at direct state censorship, but at the environment required for informed political debate in a free society by focussing on standards when it comes to video forensic evidence, and its role in truth-making. They examine in depth the forensic examination of a set of videos that purportedly show the cold-blooded shooting of Tamil Tigers

by the Sri Lankan armed forces during the civil war, and how opaque technical procedures go on to determine "truth" in political discourse.

The next chapter is that on India by Pranesh Prakash. In that chapter he presents an overview of online censorship in India since the mid-1990s, from direct state censorship to state-directed and private state-independent censorship, and then focusses on the new intermediary liability regime that brings about what he terms "invisible censorship".

Prof. Hong Xue continues with the theme of intermediary liability in China, focussing on the hugely successful e-commerce 'third-party platforms'. In it she traces the evolution of the Chinese law in this regard, thus explaining the difficulty that courts have faced of striking a fair balance between consumer protection, protection of trademark, and encouraging innovation in these online shopping malls.

Myanmar's censorship and surveillance regimes form the basis of Erin Biel's chapter, and she examines these regimes through the lens of the ethno-religious conflicts there. Her chapter shows the faultlines and the similarities between the regimes that regulate the traditional press and the digital public sphere — telecom surveillance is even easier to conduct than physical surveillance, hate speech is as readily disseminated online — using platforms like Facebook — as offline, and reporters can be arrested for challenging state corruption. It also shows that the existence of the digital sphere doesn't accomplish much in countries where the Internet penetration is low and where " government that is accustomed to maintaining state control over the media and telecommunications industries may have difficulty embracing all that freedom of the press and freedom of speech encompass."

Profs. Mônica Steffen Guise Rosina and Alexandre Pacheco da Silva study the decidedly 'old-school' means employed in Brazil by corporations and state officials to prevent their critics from challenging them. In both the cases they examine, the defendants were critics who were ordered by the judiciary to refrain from using particular online social networks to communicate their message, leading the authors to look at the importance of the infrastructure of free expression.

Rounding off the book, Dr. Nagla Rizk explores a period of approxim-

ately a week in great detail: the period in January–February 2012 when access to the Internet and various telecom services were shut down in Egypt by the authorities. She presents one of the most detailed accounts of the actual mechanism through which the blocks took place, and then examines a part of the economic impact of this outage of communication channels.

DANGERS OF NEW SCHOOL CENSORSHIP

A common theme that emerges out of this book as a whole is that in new school censorship, restrictions imposed on speech and expression, or on the infrastructures of speech and expression, do not constitute the entirety of the problem. Censorship never results in restrictions alone; it simultaneously results in the production of new discourses around the object of censorship, as well as its discursive limits.[5] As film studies scholar Annette Kuhn notes, "Censorship is not reducible to a circumscribed and predefined set of institutions and institutional activities, but is produced within an array of constantly shifting discourses, practices and apparatuses . . . [it] is an ongoing process embodying complex and often contradictory relations of power."[6] The productive nature of censorship is seen in the fact that we often create satire with which to mock censorship,[7] as well as the increased attention that which is sought to be censored gets, which on the Internet is often referred to as the "Streisand Effect".[8]

Society will never be free of censorship, nor of resistance to censorship. Indeed, the very technologies that seem to liberate our communications and form the means of our modern self-expression are the selfsame technologies that enable states and corporations greater powers of censorship and surveillance.[9] Old-school censorship, it would seem, is simultaneously both non-productive — since it often does not work well at being a restriction — as well as productive, since it often results in counter-speech, both directly critical and subversive. Citizens may not always have been able to legally challenge old-school censorship in non-democratic regimes, but they could very often see it and galvanize against it, and in many cases, subvert it in myriad ways.

There are indications that in many circumstances new-school censorship may be more effective than old-school censorship by making invisible

the fact that speech regulation is happening, and thus depriving speakers and the audience of the ability to engage with the fact of censorship and to indulge in counter-speech. Even where new-school censorship is visible, it has not always received the same treatment with respect to principles of process and court access, due to it happening mostly through private parties, and not readily being seen as 'censorship'. Thus, the constitutional safeguards that citizens in a democracy use to protect themselves against the state, are not as readily available against private entities such as internet service providers, domain name hosting services, web hosting services, and social media platforms. Given this, civic engagement with processes of censorship assumes the highest importance. However, such engagement with censorship must be studied not merely at the social and cultural levels, but must be accounted for in legal and procedural terms as well.[10]

This shift in relative importance of the actor that controls expression is also a shift that signifies the changes in state ownership of media and communications infrastructure — from the time when many governments exercised monopolies over telecommunications networks and radio stations and television channels, and some of which are still controlled by licensing regimes in many parts of the world. The advent of the Internet as a network of largely privately-owned networks, with a large part of people's daily interactions being on servers owned by private corporations, without licensing requirements in most parts of the world, further reduces the opportunities for direct state censorship. States desirous of censoring material must, for it to be effective, seek the cooperation of these private entities, as police action is far less likely to be effective. Equally, the spectre of private censorship becomes omnipresent online since private corporations — especially the ones with millions of users — now often have the regulatory reach of state, but very often do not have restrictions placed upon them in the form of the freedom of expression or privacy rights that we often enjoy against the state.

The case studies that are contained in the rest of this book bring to the forefront the legal hurdles we currently encounter and must cross if we are to ever effectively safeguard ourselves against the harms of censorship.

1 Jack Balkin, *What is Access to Knowledge?*, BALKINIZATION (Apr. 21, 2006), http://balkin.blogspot.com/2006/04/what-is-access-to-knowledge.html.

2 Jack Balkin, *Two Ideas for Access to Knowledge — The Infrastructure of Free Expression and Margins of Appreciation*, BALKINIZATION (Apr. 30, 2007), http://balkin.blogspot.in/2007/04/two-ideas-for-access-to-knowledge.html. In this, Balkin elaborates on what he means by 'infrastructure of free expression':

> *What is in that infrastructure? It includes government policies that promote the creation and delivery of information and knowledge. It concerns government policies that promote transparency and sharing of government created knowledge and data. It involves government and private sector investments in information provision and technology, including telephones, telegraphs, libraries, and Internet access. It includes policies like subsidies for postal delivery, education, and even the building of schools.*

3 *See* Derek Bambauer, *Cybersieves*, 59 DUKE L.J. 377, 384–386 (2009). Also, see generally Helen Freshwater, *Towards a Redefinition of Censorship*, *in* CENSORSHIP & CULTURAL REGULATION IN THE MODERN AGE 225 (Beate Müller, ed. 2004).

4 Jack Balkin, *Old-School/New-School Speech Regulation*, 127 HARV. L. REV. 2296 (2014), *available at* http://cdn.harvardlawreview.org/wp-content/uploads/2014/06/vol127_balkin.pdf.

5 MICHEL FOUCAULT, 1 THE HISTORY OF SEXUALITY 15–18

6 ANNETTE KUHN, CINEMA, CENSORSHIP, AND SEXUALITY 127.

7 Foucault dismisses this "illicit discourse" as less important. *See* FOUCAULT, *supra* note 5, at 18.

8 T.C., *The Economist Explains: What is the Streisand Effect?*, THE ECONOMIST (Apr. 15 2013), http://www.economist.com/blogs/economist-explains/2013/04/economist-explains-what-streisand-effect.

9 *See generally* EVGENY MOROZON, THE NET DELUSION (2011) (detailing the usage of digital technologies by authoritarian regimes). *See also* Jack Balkin, *supra* note 4, at 2304–05 ("Many of the same features of the digital infrastructure that democratize speech also make the digital infrastructure the most powerful and most tempting target for speech regulation and surveillance. Although the digital infrastructure frees speakers from dependence on older media gatekeepers, it does so through the creation of new intermediaries that offer both states and private parties new opportunities for control and surveillance.").

10 *See generally* Bambauer, *supra* note 3, at 390–410.

THE PRIVATIZATION OF FREE EXPRESSION

Laura DeNardis

Much attention to online global censorship rightly focuses on the role of sovereign nation states in enacting systems of filtering and blocking of information. Yet, governments are not able to control the global flow of information without action by private industry. The public sphere is digitally mediated and this digital architecture is primarily owned and operated by private telecommunications companies and information intermediaries. Governments wishing to enact censorship or block access to knowledge delegate this function to private companies, whether network operators, search engines, social media platforms, domain name system (DNS) registries, or financial or transactional intermediaries.

This characteristic of governments delegating content control to private sector infrastructure providers exists irrespective of the rationale for blocking, whether it is intellectual property rights enforcement or other law enforcement function or blocking political speech critical of government. The transparency reports of information intermediaries like Twitter[1] and Google[2] portray systems of information removal in which governments ask private industry to remove politically sensitive material or carry out various law enforcement requests to block information. Governments in Syria, Egypt, and elsewhere have blocked citizen access to communication systems during political turmoil. Media content companies and law enforcement increasingly view Internet service providers as mechanisms for intellectual property rights enforcement by cutting off Internet access for individuals who repeatedly infringe copyright laws.

Such instances of censorship and blocking in the digital era focus on action *originating* in the state but *delegated* to and executed by private actors. These private actors are not passive entities mechanistically executing information filtering requests but make decisions determining which government requests to oblige and which to deny. In some cases, private companies can serve as a check on government power, refusing some requests while carrying out others. Nevertheless, the censorship is born from governmental rather than private action.

In other cases, censorship originates *sui generis* in the private sphere rather than in the state, with traditional governance structures having no part in either initiating or carrying out censorship. Private entities like Twitter have made decisions to delete certain accounts; private citizens use distributed denial of service (DDoS) tools take down web sites. Apple removes apps it deems controversial; financial intermediaries block the flow of funds to sites as they did after WikiLeaks released United States' diplomatic cables. The criteria by which private companies delete information or accounts are delineated to a certain extent in terms of service agreements, but many decisions involve ad hoc subjective decisions.

American constitutional law scholar Jack Balkin has often explained that conceptions of freedom of expression are over-relegated to concerns about negative liberties such as preventing government censorship, while true access to knowledge depends on a broader "infrastructure of free expression" ranging from investments in information technology, policies that promote information sharing, and certain constructions of intellectual property laws.[3]

This chapter extends this theory of access to knowledge into the realm of infrastructures of Internet governance, and in particular, concerns about emerging forms of infrastructure design and administration on access to knowledge. Thus, this chapter explores several infrastructure-mediated structures in which private Internet governance actors determine freedom of expression: *sui generis private censorship* in which information blocking originates in and is executed by private ordering; *discretionary and delegated censorship* in which private information intermediaries adjudicate which government-delegated censorship requests to oblige and which to refuse; and i*nfrastructures of free expression* in which Internet archi-

tecture design and coordination can directly promote or impede possibilities for access to knowledge and expressive freedom.

New forms of private infrastructures of Internet governance create new possibilities for technical expediency, advancements in innovation, and access knowledge. But they also require public scrutiny to assess the potential consequences to innovation, infrastructure, and civil liberties. The chapter concludes with an examination of the implications of the privatization of Internet governance for the future of free expression and Internet stability and the need to preserve technical characteristics of universality, interoperability, openness, and anonymity.

PRIVATE MEDIATION OF CENSORSHIP

Google's informal motto is "Don't be Evil".[4] The mere existence of this slogan signals the recognition that information intermediaries have the power to "be evil" and that this is something with which companies struggle in various political and economic contexts around the world. Information intermediaries are private platforms that do not create content themselves but rather facilitate content transactions between those entities that provide or access this content. They manipulate, store, sort, rate, aggregate, or otherwise provide an information mediation function of value for Internet users. Prominent examples include search engines, content aggregation sites, and social media platforms. Other types of information intermediaries provide financial or transactional services around the content, such as facilitating payments or commerce.

These companies determine conditions of freedom of expression at many levels. Private intermediaries receive a constant barrage of government requests to remove information. In these cases of delegated censorship, the transparency reports of private companies indicate that they are not passively acquiescing to any government request but provide some sort of determination about what to censor and what not to censor. This determination *is* governance, with private companies playing a gatekeeping function between the state and private citizens. In other cases, private companies enact discretionary censorship in which a request to block or remove information or accounts does not originate with the state but in private ordering. The private choice to delete content can originate in the values embedded in end user agreements, in cultural and political norms,

in anti-competitive behaviour, or in concern about reputational harm certain content can effect. This section provides representative cases of the various roles private ordering plays in determining conditions of censorship and freedom of expression online.

SUI GENERIS PRIVATE CENSORSHIP

During the London Olympic Games in 2012, Twitter suspended the personal account of a journalist serving as a correspondent for the British newspaper the *Independent*. The reporter had posted several tweets critical of NBC's coverage of the games, including one that called for the public to email complaints to an NBC executive. Twitter initially claimed that NBC requested that the journalist's account be terminated because the account owner had published the email address of the NBC executive. The suspension of the journalist's Twitter account was met with a considerable public backlash online, in part because many believed the action was motivated somewhat by Twitter's cross-promotional Olympics partnership with NBC.[5] Twitter ultimately restored the journalist's account and its General Counsel admitted that it was actually a Twitter employee, rather than an NBC employee, that proactively monitored the content and originally identified what he considered to be the objectionable tweet.[6] In this case, it was not only the content that was taken down, but the journalist's entire account.

A similar function of private Internet governance involves decisions about what third-party developed smartphone and tablet applications (known in this context as "apps") to make available in privately run app stores. Legal scholar Jonathan Zittrain has expressed concerns about the transformation from computing environments in which individuals have the choice of types of applications to use on their computing devices to mediated environments in which device gatekeepers determine which applications, and therefore, what associated content, users can access.[7] In the smart phone and tablet market, for example, Apple exerts control over which third-party developed apps appear in its App Store and Google exerts control over the apps it allows provided for the Android platform. The companies that operate app stores publish developer guidelines designed to define the conditions under which apps will be rejected or removed. Some of these guidelines specify technical requirements related to

functionality, interoperability, and bandwidth constraints, such as prohibitions of any apps larger than 20 MB from downloading over a cellular network. Many developer guidelines also attempt to address content limitations.

Criteria for rejecting apps for objectionable material are somewhat vague. Apple, for example, makes it clear that it will reject Apple Apps that are "over the line" but describing this line is very difficult. Apple's app developer guidelines explain that defamatory or mean-spirited apps that place a targeted individual in danger will be rejected, as will any application portraying realistic depictions of people or animals being killed. In some cases, apps are removed after already being included in the App Store, such as Apple's decision to remove a Hezbollah-related application.[8] But guidelines are interpretively subjective enough to provide companies with broad discretion to reject any apps it deems not appropriate. For example, Apple originally accepted an unofficial WikiLeaks app into its store but removed it after several days, claiming broadly that it was in violation of developer guidelines.

As Apple's "App Store Review Guidelines" state:

> *We view Apps different than* (sic) *books or songs, which we do not curate. If you want to criticize a religion, write a book. If you want to describe sex, write a book or a song, or create a medical app. It can get complicated, but we have decided to not allow certain kinds of content in the App Store.*[9]

Apple similarly removed an independently-developed "Phone Story" app, a game themed around abject smart phone factory conditions and worker suicides.[10] In this regard, information that is app-mediated is subject to much greater speech restrictions than information accessible on the open Web via a browser. When a company restricts or removes an app from its store, it is not only the app that is blocked but the information potentially made available via that app. Hundreds of thousands of apps are provided in various mediated repositories, an environment that promotes innovation, new products, and user satisfaction. However, freedom of expression in these environments is determined by private gatekeepers, raising concerns about such privatization of individual rights. Because the prevailing app-mediated architecture involves private gatekeepers determ-

ining what is and is not objectionable, some scholars are calling for the industry application of principles of "app neutrality" involving unambiguous developer guidelines, a clear explanation for why apps are rejected, and a transparent appeals process.[11]

There are similar cases of transactional and financial intermediaries cutting off transactions or the flow of currency to an online site without direct governmental prodding to do so. Perhaps the most well-known instance of such private governance occurred when Amazon cited its terms of service as justification for suspending its web hosting of WikiLeak's web sites after WikiLeaks during the so-called Cablegate incident. An official Amazon statement explained that its decision to cease providing hosting services was not a result of a government request.[12] Financial intermediaries, including PayPal, also ceased providing services to WikiLeaks.[13] PayPal similarly stated that the company was not contacted by any government organization but came to the decision to cut off the flow of funds to WikiLeaks based on their Acceptable Use Policy and after the United States Department of State indicated that the WikiLeaks information release violated U.S. law.[14]

These examples of private Internet governance, whether terminating an account, blocking an app, removing particular information, or cutting off the flow of funds to an online site, indicate the power information intermediaries have over who has the right to speak in the digital public sphere.

PRIVATE INDUSTRY MEDIATION OF DELEGATED CENSORSHIP

Governments are rarely able to autonomously remove or block online content but must approach an informational or infrastructural intermediary to do so. These private intermediaries receive a constant barrage of removal requests. Some of these requests involve blatant or cultural censorship while some are attempts to enforce nation-specific laws about everything from defamation and child protection to national security and state secrets. Content-related laws vary enormously from country to country. For example, Thailand has severe *lèse-majesté* laws criminalizing insulting a monarch and has imprisoned citizens for such speech online.[15] Brazilian and Dutch laws include strong prohibitions against hate speech. Germany and Israel have statutes prohibiting the dissemination of Holo-

caust denials and Nazi propaganda. Private companies receiving information take down requests face an intractable task of determining which requests to oblige and which to deny across heterogeneous cultures and regulatory systems.

The number of government content removal requests private companies receive has steadily increased. For example, the number of content removal requests Google received from the Brazilian government during the July to December 2012 reporting period increased 265% from the previous six-month period.[16] Many government requests address specific issues such as defamation, impersonation, and hate speech. In other cases, the company interprets requests as political censorship. As a Google blog post accompanying one of its transparency reports notes, ". . . just like every other time before, we've been asked to take down political speech. It's alarming not only because free expression is at risk, but because some of these requests come from countries you might not suspect — Western democracies not typically associated with censorship."[17]

Based on limited data from private industry disclosures about government content removal requests, many multinational companies do not just passively remove targeted information any time a government makes such a request (although some do in parts of the world). Instead, they perform a governance function in determining which requests to carry out and which to refuse. Google's Transparency Reports are quite telling in this regard. Looking at overall percentages, and in the reporting period covering January to June 2013, the company complied with 54% of court orders globally and 27% of non-court (executive, police) requests.[18] For example, Google declined most government requests to delete the controversial "Innocence of Muslims" video, although temporarily blocking access in certain areas.[19]

The following provides an excerpt from the Google Transparency Report, this one referring to Brazilian government requests, and helping to convey the types of requests intermediaries receive and the response of private companies in pushing back against some of these requests:

> *We received 316 requests for the removal of 756 distinct pieces of content related to alleged violations of the Brazilian Electoral Code during the 2012 Brazilian Elections. Google removed content in response to 35 final court*

decisions. Google is exercising its right of appeal provided under Brazilian law in the other cases, on the basis that the content is protected by freedom of expression under the Brazilian Constitution.
We received a request from a federal prosecutor to remove five blog posts and four search results linking to blog posts that allegedly defame him by accusing him of incompetence and corruption. We did not remove content in response to this request.
We received a request from one judge to remove a blog that allegedly defamed him by referencing or linking to accusations of corruption, and a similar request from a different judge to remove a search result. We did not remove the blog or the search result.[20]

Information intermediaries are subject to the laws in the jurisdictions in which they do business, but also exercise discretion about the requests with which they comply. This is not the case in all contexts. Some technology companies have little or no discretionary power to refuse government content removal requests, such as search engine giant Baidu in carrying out requests the Chinese government makes to remove search terms and block uniform resource locators.

Delegated censorship is not at all relegated to platform intermediaries like search engines and social media platforms but descends into infrastructures designed exclusively to perform some function of Internet governance. The prime example of the turn to infrastructures of Internet governance for content control involves the Internet's domain name system (DNS). The DNS was designed to perform a straightforward technical task: it serves as the universal directory that authoritatively translates between the alphanumeric domain names (such as bbc.co.uk) that humans use to access the Internet and the numeric Internet Protocol (IP) addresses that routers use to forward packets of information to their appropriate destination. This system is a fundamental mechanism that keeps the Internet operational and that is designed to maintain the global universality of the Internet. In other words, someone wanting to access bbc.co.uk can reach the same site whether typing in that domain name in South Africa, Argentina, or the United Kingdom.

Although the function of Internet naming and translation is quite straightforward, the DNS is actually a technologically massive and com-

plex database system distributed across numerous servers located around the world. The DNS is the epitome of modern 'big data' systems, processing hundreds of billions of queries each day, and administered by a multifaceted global institutional framework, including the Internet Corporation for Assigned Names and Numbers (ICANN), the Internet Assigned Numbers Administration (IANA), and dozens of registries and thousands of registrars. It is also a system whose operational function instantiates numerous public policy issues ranging from Internet security and stability to equitable resource distribution to domain name trademark disputes. In other words, it is a complicated technical and public policy area without being used for content filtering.

As summarized by a group of prominent Internet engineers, "Strong governments around the world use DNS filtering to signal their displeasure over all kinds of things they don't like, whether it be untaxed online gambling, or pornography, or political dissent."[21] The DNS, although distributed across servers and delegated hierarchically to various institutions creates central points of control for blocking access to content. It is both necessary for the Internet to function and a centralized control point. Domain names can be de-registered; queries of domain names into IP addresses can be filtered or redirected. This is not a hypothetical phenomenon, but a content-control technique that has been deployed for censorship as part of the so-called 'great firewall of China', for intellectual property rights enforcement by the Immigration and Customs Enforcement (ICE) agency of the United States' Department of Homeland Security, in the proposed American legislation known as the Stop Online Piracy Act (SOPA), and several other global initiatives. The registries and registrars asked to carry out these content blocking techniques can do so if the request originates with a foreign government but have much less recourse if the request comes from the government in the jurisdiction in which they physically operate.

INFRASTRUCTURE AND FREE EXPRESSION

These examples of private infrastructure-based adjudication of censorship help raise a different set of questions about the relationship between characteristics of privatized infrastructure and possibilities for freedom of expression. Private industry mediates between governments and citizens

and makes direct decisions about the global flow of information and therefore about expressive and economic liberty. While private infrastructure and platforms have fuelled global Internet growth and innovation, the increasing public policy role of these intermediaries in determining public policy — whether over surveillance revelations or issues of free speech — is attracting broad attention to prevailing Internet governance frameworks.

Internet governance generally refers to the design and administration of the technologies necessary to keep the Internet operational and the enactment of public policy around this architecture. In addition to the platform and infrastructure intermediary functions already mentioned, other, more technically concealed infrastructural control areas of Internet governance and administration are similarly privatized. While nation states and intergovernmental agreements have prominent Internet governance roles in areas as diverse as antitrust oversight, computer fraud and abuse, child protection, defamation, privacy, and intellectual property rights enforcement, a significant part of day-to-day operational aspects of Internet control are enacted by the private sector and private, non-profit institutions. Private companies serve as Internet registries and operators running the domain name system; employees of private companies contribute most technical standards work; private infrastructure providers carry out cybersecurity governance; network operators executive private contractual agreements to interconnect to form the global Internet; ICANN and the regional Internet registries distribute names and numbers. All of these functions, along with platform intermediaries, keep the Internet operational and, effectively, establish public policy for the Internet.

As Internet governance debates increasingly enter the policy making and public discourse, questions about the legitimacy and implications of these forms of private public policy will also increase. All of these concerns will relate to infrastructure design and administration. Will there be a resurgence of proprietary values commensurate with pre-ARPANET/INTERNET contexts? Will Internet control points be used for competitive advantage and information enclosure? Will newer forms of architectural arrangements, like cloud computing, have the same interoperability and openness as traditional Internet applications like web access, email, and file transfer? Is there adequate accountability and transparency in private

arrangements like interconnection? Do network management techniques like deep packet inspection compromise individual privacy? Are traffic prioritization mechanisms solving network management problems or being used for competitive advantage? Will DNS filtering compromise the Internet's security and stability?

These questions and the values at stake will likely serve as invitations for greater public and government scrutiny of Internet governance, as has recently been seen in the efforts of some countries to increase intergovernmental influence on Internet coordination functions, and in the NETMundial global multistakeholder meeting on Internet governance convened in April 2014 in Brazil, in part as a response to Edward Snowden's exposure of widespread NSA surveillance. Greater government involvement is not necessarily a solution in the fast-paced Internet environment, so it is critical that private actors establish procedures that support the multistakeholder accountability and transparency norms of the Internet. The legitimacy of increasingly privatized governance is contingent upon the preservation and promotion of certain technical characteristics providing infrastructures of free expression.

Some of these characteristics include interoperability, openness, universality, infrastructure stability and the technical possibility for online anonymity. Unfortunately, there are forces that are moving the Internet away from these norms. One challenge is the erosion of possibilities for anonymity, a characteristic historically necessary for democratic expression. This shift is occurring both at the content and application level and within intermediating infrastructures. Some social media policies and news commentary spaces require real name identifiers. Cybercafés increasingly require the presentation of identification cards. Online advertising business models are predicated upon the collection of unique technical identifier fingerprints involving unique hardware addresses, virtual IP addresses, locational information, software configurations, and all manner of metadata associated with smartphones and tablets. The existence of this entrenched identity infrastructure beneath the layer of content makes it challenging to achieve real anonymity. Whether the possibility of anonymous speech will ever again exist is at stake in global debates at the platform, device, and infrastructure level.

There is a similar movement away from interoperability and universality. While there is more connectivity than ever before at the usage level, there is sometimes less interoperability, no longer an inherent goal of companies developing products and applications for the Internet. Some platforms are designed specifically using proprietary protocols; gatekeepers are controlling the flow of apps rather than applications residing at end points and under user control; voice over Internet platforms are often interoperable without special billing arrangements; and universal search is eroding. Gatekeeping approaches have market inertia, but could have considerable long term Internet functionality and governance implications. Movements toward using the DNS for enforcing intellectual property rights and other content filtering could also move the Internet toward greater balkanization.

Technical architecture is not fixed any more than Internet governance is fixed. While the same technologies that create advancements in access to knowledge also can be used for surveillance and restrictions on knowledge, there are some characteristics of technical architecture that are necessary for the ongoing prospect of freedom of expression. The extent to which private ordering promotes these forms of technical architecture, as well as adopts values of transparency and multistakeholder participation, will determine whether the balance of Internet governance requires global transformation.

1 TWITTER TRANSPARENCY REPORT, https://transparency.twitter.com/ (last visited June 2, 2014).

2 GOOGLE TRANSPARENCY REPORT, http://www.google.com/transparencyreport/ (last visited August 10, 2014).

3 *See, e.g.*, Jack Balkin, *Two Ideas for Access to Knowledge — The Infrastructure of Free Expression and Margins of Appreciation*, BALKINIZATION (Apr. 30, 2007), http://balkin.blogspot.com/2007/04/two-ideas-for-access-to-knowledge.html (Balkin's inaugural address at the Second Access to Knowledge Conference (A2K2) at Yale Law School).

4 *Code of Conduct — Investor Relations*, GOOGLE, http://investor.google.com/corporate/code-of-conduct.html (last visited June 2, 2014).

5 *See* Press Release, NBC Sports Group, *NBC Olympics and Twitter Announce Partnership for London 2012 Olympics Games* (July 23, 2012), http://www.nbcuni.com/corporate/newsroom/nbc-olympics-and-twitter-announce-partnership-for-london-2012-olympic-games/

6 Alex Macgillivray, *Our Approach to Trust & Safety and Private Information*, TWITTER BLOGS (July 31, 2012), http://blog.twitter.com/2012/07/our-approach-to-trust-safety-and.html.

7 *See generally* JONATHAN ZITTRAIN, THE FUTURE OF THE INTERNET AND HOW TO STOP IT (2008).

8 *See* Press Release, Anti-Defamation League, *ADL Praises Apple for Removing Hezbollah TV App from iTunes Stores* (July 31, 2012), http://archive.adl.org/presrele/internet_75/6353_75.html.

9 *App Store Review Guidelines*, APPLE DEVELOPER, https://developer.apple.com/app-store/review/guidelines/ (last visited August 10, 2014).

10 Mark Brown, *Apple Bans* Phone Story *Game That Exposes Seedy Side of Smartphone Creation*, WIRED (Sept. 14, 2011), http://www.wired.com/2011/09/phone-story/.

11 *See, e.g.*, Luis Hestres, *App Neutrality: Apple's App Store and Freedom of Expression Online*, 7 INT'L J. COMM. 1265 (2013), *available at* http://ijoc.org/index.php/ijoc/article/view/1904.

12 *WikiLeaks*, AMAZON WEB SERVICES (Dec. 3, 2010), http://aws.amazon.com/message/65348/.

13 *PayPal Statement Regarding WikiLeaks*, PAYPAL BLOG (Dec. 3, 2010), https://www.thepaypalblog.com/2010/12/paypal-statement-regarding-wikileaks/, *archived at* http://archive.today/plqY2; *see also* Kevin Poulsen, *PayPal Freezes WikiLeaks Account*, WIRED (Dec. 4, 2010), http://www.wired.com/2010/12/paypal-wikileaks/.

14 John Muller, *Updated Statement about WikiLeaks from PayPal General Counsel*, PAYPAL BLOG, (Dec. 8, 2010), https://www.thepaypalblog.com/2010/12/updated-statement-about-wikileaks-from-paypal-general-counsel-john-muller/, *archived at* http://archive.today/BikQ.

15 *See, e.g., Thailand's Lèse-Majesté Laws: An Inconvenient Death*, THE ECONOMIST (May 12, 2012), http://www.economist.com/node/21554585 (describing the imprisonment and death of Ampon Tangnoppakul for allegedly sending SMSes that violated Thailand's *lèse-majesté* laws, despite his plea that he didn't even know how to send SMSes.)

16 *See Notes*, GOOGLE TRANSPARENCY REPORT, http://www.google.com/transparencyreport/removals/government/notes/ (last visited August 10, 2014).

17 Dorothy Chou, *More Transparency into Government Requests*, OFFICIAL GOOGLE BLOG (June 17, 2012), http://googleblog.blogspot.com/2012/06/more-transparency-into-government.html.

18 *Government Removal Requests*, GOOGLE TRANSPARENCY REPORT, http://www.google.com/transparencyreport/removals/government/?metric=compliance (last visited August 10, 2014).

19 Claire Cain Miller, *As Violence Spreads in Arab World, Google Blocks Access to Inflammatory Video*, N.Y. TIMES, Sept. 13, 2012, at A12, *available at* http://www.nytimes.com/2012/09/14/technology/google-blocks-inflammatory-video-in-egypt-and-libya.html?_r=0.

20 *Notes*, *supra* note 16.

21 Paul Vixie et al., *Mandates Can't Alter Facts*, THE HILL - CONGRESS BLOG (Dec. 14, 2011), http://thehill.com/blogs/congress-blog/technology/199435-mandates-cant-alter-facts

UNITED STATES OF AMERICA

THE RISE OF INDIRECT CENSORSHIP

Anjali Dalal

Censorship is traditionally understood as a direct prohibition on speech. However, indirect censorship, which deters individuals from engaging in speech that is not explicitly prohibited, chilling otherwise-protected speech, is also a form of censorship. Laws that discourage free speech allow the government to indirectly control the words spoken, friends kept, and religions practised by the public. Such government-induced self-censorship is equally, if not more, invidious as direct prohibitions on speech.

One early example of indirect censorship in the USA was a law that required public school teachers to take a loyalty oath denying affiliation with "any agency, party, organization, association, or group . . . determined by the United States Attorney General or other authorized agency of the United States to be a communist front or subversive organization."[1] In *Wieman v. Updegraff*, the Supreme Court acknowledged the "perennial problem" of defining the relationship between a government and a free society during "periods of international stress," but ultimately found that a program in which "disloyalty is screened by ideological patterns"[2] was unconstitutional because "membership may be innocent"[3] and "to thus inhibit individual freedom of movement is to stifle the flow of democratic expression and controversy at one of its chief sources."[4] The Court expressed a concern that such a law had "an unmistakable tendency to chill

that free play of the spirit which all teachers ought especially to cultivate and practice."[5] With these words, the Supreme Court formally introduced what became, over the next 20 years, a "major substantive component of First Amendment adjudication"[6]: the chilling effects doctrine.

However, the chilling effects doctrine is no longer front and centre in First Amendment[7] adjudication. Since the 1970s, the composition and legal disposition of the Supreme Court has changed, resulting in the weakening of the chilling effects doctrine as powerful legal tool to combat indirect government censorship. In its wake, the U.S. has experienced a growth of a specific form of indirect government censorship: surveillance. Compared to the loyalty oaths of the mid-twentieth century, today's chilled speech is the product of mass, blanket surveillance of both the public and private spheres.

This chapter will discuss the evolution of the chilling effects doctrine and describe the government surveillance that it has facilitated.

THE EVOLUTION OF THE CHILLING EFFECTS DOCTRINE

In 1972, the brakes were slammed on the quickly evolving chilling speech doctrine. The Supreme Court was presented with a case contesting the propriety of Army surveillance of Americans in the wake of the race riots spreading across the country after the assassination of civil rights leader, Dr. Martin Luther King, Jr.[8] The public was informed of this otherwise secret surveillance program through an article in *The Washington Monthly*, which revealed that the Army was actively collecting information on the public activities and meetings of American persons who were deemed to pose a threat of civil disorder.[9] In addition to gathering information on their own, the Army was working with civilian law enforcement agencies to refine the corpus of information they were developing.[10]

Arlo Tatum, the Executive Secretary of the Central Committee for Conscientious Objectors, brought suit against the government, along with similarly situated plaintiffs, claiming that the surveillance practices chilled their political speech and impermissibly violated their First Amendment rights.[11] However, importantly, neither Tatum nor the other plaintiffs had evidence that they were subject to the allegedly impermissible surveillance.[12]

When addressing their First Amendment claim, *Laird* held that the "speculative apprehensiveness that the Army may at some future date misuse the information in some way that would cause direct harm to respondents" did not constitute the sort of "objective harm or threat of specific harm" that the Court was constitutionally permitted to consider.[13] The Court held that "the mere existence . . . . of a governmental investigative and data-gathering activity that is alleged to be broader in scope than is reasonably necessary for the accomplishment of a valid governmental purpose" did not present a judicially cognizable injury.[14] In so holding, *Laird* effectively required an individual seeking to raise a First Amendment claim against the broad sweep of government surveillance to first prove that she has been subject to and harmed by the often-covert surveillance.

Laird cut against the Court's earlier decision in *Dombrowski v. Pfister*,[15] which had expanded standing doctrine in chilling effects cases. *Dombrowski* recognized the "sensitive nature of constitutionally protected expression," and, as a result, did not require "all of those subject to overbroad regulations risk prosecution to test their rights," worried that in holding otherwise, "free expression—of transcendent value to all society. . .might be the loser."[16] The *Dombrowski* Court established such an exception to the traditional rules of standing because the alterative would leave "the contours of regulation . . .[to] be hammered out case by case—and tested only by those hardy enough to risk criminal prosecution to determine the proper scope of regulation."[17] Contrary to the spirit of *Dombrowski*, *Laird* demands that a plaintiff first prove that she is personally subjected to and objectively harmed by government surveillance before she is able to surpass the standing barriers put in place by the Supreme Court.

The premise of *Laird* has since been affirmed and expanded. In *American Civil Liberties Union v. National Security Agency*, the Sixth Circuit ruled that the ACLU lacked standing to sue the government after it was discovered that "President Bush authorized the NSA to begin a counter-terrorism operation...which include[d] the interception (i.e., wiretapping), without warrants, of telephone and email communications where one party to the communication is located outside the United States and the NSA has a reasonable basis to conclude that one party to the communication is a member of al Qaeda, affiliated with al Qaeda, or a member of an organization affiliated with al Qaeda, or working in support of al

Qaeda."[18] In *ACLU v. NSA*, the court emphasized that the plaintiffs failed to "allege as injury that they *personally*, either as individuals or associations, anticipate or fear any form of direct reprisal by the government (e.g., the NSA, the Justice Department, the Department of Homeland Security, etc.), such as criminal prosecution, deportation, administrative inquiry, civil litigation, or even public exposure."[19] The court found that "'chilling' is not sufficient restraint no matter how valuable the speech,"[20] and held that plaintiffs failed to allege a judicially cognizable claim because they did not "establish that [they were] . . . regulated, constrained, or compelled directly by the government's actions, instead of by [their] . . . own subjective chill."[21]

In 2008, elements of the warrantless wiretapping program initiated by President Bush were legalized through the FISA Amendments Act of 2008,[22] and organizations and individuals came together to sue the government arguing that there was, based on the language of the statute, an objectively reasonable likelihood that their communications in particular would be subject to government surveillance in violation of their constitutional rights. In *Clapper v. Amnesty International*, the Supreme Court held that those organizations and individuals who were, by the letter of the law, likely to be unfairly caught up within a congressionally-authorized surveillance program because of their role as "attorneys and human rights, labor, legal, and media organizations" working with "sensitive and sometimes privileged telephone and e-mail communications with colleagues, clients, sources, and other individuals located abroad" were nonetheless alleging a speculative harm and thus did not qualify for standing to litigate the constitutionality of the statute in question.[23] The Court held that respondents' theory of injury arising from their likelihood of being subject to surveillance and needing to take costly measures to protect the safety of their clients, sources and colleagues abroad is "too speculative to satisfy the well-established requirement that threatened injury must be 'certainly impending'."[24] The U.S. government has argued strongly in favour of erecting extra strong standing barriers, stymying litigation alleging the unconstitutionality of national security programs, even when Americans are able to offer evidence of dragnet government surveillance. In *Jewel v. National Security Agency*, the plaintiff class was finally able to offer evidence of government wiretaps on AT&T's customers that occurred during the Bush

Administration.[25] The evidence, provided by former AT&T telecommunications technician Mark Klein, showed that AT&T routed copies of Internet traffic to a secret room in the Folsom Street facility in San Francisco that was controlled by the NSA. The government argued and the district court agreed that the "political process, rather than the judicial process" was the appropriate avenue for raising concerns about national security efforts.[26] Furthermore, the government argued, and the district court again agreed, "the reluctance to adjudicate constitutional questions is heightened when, as here, the constitutional issues at stake in the litigation seek judicial involvement in the affairs of the executive branch and national security concerns appear to undergird the challenged actions."[27]

While the Ninth Circuit ultimately rejected the government's argument and overturned the district court's decision in *Jewel*, there is no denying that judicial doctrine has evolved in a way that extricates the courts from national security based surveillance cases. As I have discussed in previous work, even judges recognize the problems with the current system.[28] For example, Judge Colleen McMahon wrote in a recent court opinion, "The Alice-in-Wonderland nature of this pronouncement is not lost on me; but after careful and extensive consideration, I find myself struck by a paradoxical situation in which I cannot solve a problem because of contradictory constraints and rules — a veritable Catch-22. I can find no way around the thicket of laws and precedents that effectively allow the executive branch of our government to proclaim as perfectly lawful certain actions that seem on their face incompatible with our Constitution and laws while keeping the reasons for their conclusion a secret."[29]

By requiring evidence of often-secret surveillance to surpass the standing barriers constructed by the courts, the chilling effects doctrine has been rendered impotent. It can no longer keep overly broad, speech-inhibiting government activities in check, which has particularly dangerous consequences in the national security context. Without judicial intervention, we have witnessed an expansion of unregulated government surveillance. The balance of this chapter will explore a few programs that illustrate this growth.

THE GROWTH OF MASS SURVEILLANCE

Though the United States does not formally authorize the existence of a domestic intelligence gathering agency, the FBI increasingly engages in domestic intelligence gathering. For example, the Attorney General Guidelines, which constitute the main source of the FBI's authority, outlining the FBI's operational policies and procedures, illustrate the growth of mass surveillance.[30]

Immediately after the September 11th attacks, new Guidelines were issued by Attorney General John Ashcroft authorizing the FBI to engage in surveillance of public gatherings and meetings "on the same terms and conditions as members of the public generally", *i.e.*, without any checks or balances.[31] The FBI was no longer required to first obtain approval from FBI headquarters and notify the Department of Justice of their activity as long as the agents were operating for the purpose of detecting or preventing terrorist activities.[32] Furthermore, the Ashcroft Guidelines allowed the FBI to "purchase detailed profiles compiled by the data mining companies without any evidence supporting suspicion," and "store this information for future investigatory purposes indefinitely."[33]

In 2008 Attorney General Michael Mukasey further expanded surveillance authority by creating an "Assessment" level of investigation, authorizing FBI agents to conduct a limited investigation on a U.S. person with no predicate factual evidence.[34] Under this new form of investigative authority, with little more than a hunch, the FBI can:[35]

1. Obtain publicly available information.
2. Access and examine FBI and other Department of Justice records, and obtain information from any FBI or other Department of Justice personnel.
3. Access and examine records maintained by, and request information from, other federal, state, local, or tribal, or foreign governmental entities or agencies.
4. Use online services and resources (whether nonprofit or commercial).
5. Use and recruit human sources in conformity with the Attorney General's Guidelines Regarding the Use of FBI Confidential Human Sources.

6. Interview or request information from members of the public and private entities.
7. Accept information voluntarily provided by governmental or private entities.
8. Engage in observation or surveillance not requiring a court order.
9. Obtain grand jury subpoenas for telephone or electronic mail subscriber information.

This massive information gathering initiative has very real consequences. For example, the FBI is authorized, pursuant to a presidential directive, to administer the Terrorism Screening Center ("TSC") which is responsible for managing the Terrorist Screening Database ("TSDB"), the federal government's centralized watchlist of known and suspected terrorists, including the No-Fly and Selectee Lists which impact an individual's ability to travel within and outside of the United States.[36] In one recent case, Rahinah Ibrahim, a citizen of Malaysia legally residing in the United States from 2001 to 2005 as a Ph.D. student at Stanford University, was allegedly wrongfully placed on the "No-Fly List" and other terrorist watchlists. She left the United States to attend a Stanford-sponsored conference where she presented her doctoral research in 2005 and has not been permitted to return to the United States since.[37] She is currently pursuing litigation to vindicate her travel rights and shed light on the ways in which individuals are placed on these government watchlists, but there are undoubtedly chilling effects of this sort of government action, especially among international academics.

State and local police are also beginning to take a more surveillance-based approach to policing. The New York City Police Department has been called "one of country's most aggressive domestic intelligence agencies" outfitted with a well-funded police department and state of the art technology.[38] NYPD undercover officers are often sent into "identified neighborhoods to isolate what the NYPD called 'hot-spots': restaurants, cafes, halal meat shops and hookah bars" across New York City and its surrounding areas in order to survey the population, collect information, and recruit informants.[39] NYPD's Assistant Chief Thomas Galati testified that speaking languages prominent among Muslim populations, including Urdu and Arabic, was sufficient to trigger NYPD surveillance.[40]

Furthermore, New York City boasts a brand new "Domain Awareness System" that "aggregates and analyses existing public safety data streams in real time, providing NYPD investigators and analysts with a comprehensive view of potential threats and criminal activity."[41] The Domain Awareness System connects with the City's "approximately 3,000 Closed-Circuit TV cameras" in addition to a plethora of other city, state, federal, commercial, and public data sources. The new program allows NYPD surveillance to "track where a car associated with a suspect is located, and where it has been in past days, weeks or months" and "map criminal history to geospatially and chronologically reveal crime patterns."[42]

To coordinate the information gathered at local, state and federal levels, the government has started to fund the creation of 'fusion centres'. Fusion centres have been called "police intelligence units on steroids",[43] but they have been formally defined as "a collaborative effort of two or more agencies that provide resources, expertise, and information to the centre with the goal of maximizing their ability to detect, prevent, investigate, and respond to criminal and terrorist activity."[44] In other words, fusion centres operate by aggregating local, state, federal, and commercial databases and other sources of information in an effort to more comprehensively analyse all available data and identify potential terrorist and criminal activities before they happen. The centres are funded by the federal government and operated by local and state law enforcement efforts.[45] There are over forty intelligence fusion centres across the country and they have quickly become a "central node" in counter-terrorism efforts.[46]

The surveillance practices described above are intended to illustrate the increasingly public nature of mass government surveillance. Despite this, the judicial backdrop against which it operates threatens to render these surveillance practices completely unassailable under the law. As a result, the chilling effects of over-broad government surveillance are inevitable, altering the way we Americans interact with our federal government, our local police force, the companies with which we share our private information, and most of all, the way we interact with each other.

The effects of mass surveillance have been studied in a recent report on the NYPD's surveillance of Muslim communities in and around New York City. While the First Amendment guarantees individuals the right to

freely practice any religion they choose, many New Yorkers have expressed a desire to avoid being identified as Muslim. The study reports that almost all of those interviewed "noted that appearing Muslim, or appearing to be a certain type of Muslim, invites unwanted attention or surveillance from law enforcement," discouraging many from growing beards, wearing certain clothes and affiliating with cultural organizations and individuals.[47]

The NYPD's "emphasis on indicators of religiosity as hallmarks of radicalization, and on religious spaces as generators of radicalization, has put the very practice of religion at the center of the NYPD's counterterrorism policing" leading one Muslim student at Brooklyn College to note, "It's as if the law says: the more Muslim you are, the more trouble you can be, so decrease your Islam."[48] Another young man notes that after he was visited by two NYPD Intelligence Division detectives and questioned at length about his online activities, though he "used to go to the masjid [mosque] quite a lot . . . [he] stopped as soon as they [the NYPD] knocked on the door."[49]

In addition to chilling religious practice, this surveillance has fostered isolation among Muslims in the New York area. The NYPD's "broad-based surveillance" turned "religious spaces, intended to provide a haven for new and old congregants to forge bonds and support networks, into the opposite — a space where interactions have become marred by mutual suspicion," with individuals expressing interest in Islam viewed with suspicion and fear.[50] As one man stated, "If a new person shows up at the mosque, everyone's eyes and ears are on the person," discouraging the creation of an open, thriving community.[51]

Wanting to avoid political discussion that might attract unwanted attention, some business owners in heavily Muslim populated areas have "consciously taken steps to avoid political discussion by muting, or completely banning, popular news channels."[52] As one such owner noted, "I don't allow Al-Jazeera on in our hookah bar. Particularly when things flare up in the Middle East. We can't control what people start saying in response to the news, and we never know who else is in the bar listening."[53]

CONCLUSION

Censorship is a global disease that manifests in different ways in different countries. In the United States, government censorship is taking the form of self-imposed censorship, inspired by the mass government surveillance that is becoming part of our daily lives. In his dissent in *Laird*, Justice Douglas recalled that James Madison, one the country's founding fathers, held a deep-seated fear that national security interests would grow to subordinate individual civil liberties, stating, "'The veteran legions of Rome were an overmatch for the undisciplined valor of all other nations, and rendered her the mistress of the world . . . . Not the less true is it, that the liberties of Rome proved the final victim to her military triumphs; and that the liberties of Europe, as far as they ever existed, have, with few exceptions, been the price of her military establishments.'"[54]

Recently, however, there have been a number of important developments, facilitated in part by the disclosures of Edward Snowden. Armed with evidence of nearly comprehensive surveillance of telephone metadata, plaintiffs are finally able to surpass the standing barrier and as of this writing, have brought lawsuits that have resulted in two different district court decisions — one finding that the bulk collection of telephone metadata was unconstitutional,[55] and the other finding the same programme to be constitutional.[56] Furthermore, the government has, for the first time, notified a criminal defendant, Jamshid Muhtorov, that evidence obtained from a warrantless wiretap will likely be used against him. The disclosure is expected to "set up a Supreme Court test of whether such eavesdropping is constitutional."[57]

Regardless of their outcomes, these cases will hopefully usher in a new and permanent change to surveillance practices in the United States: proper judicial review of surveillance programs.

1 Wieman v. Updegraff, 344 U.S. 183, 186 (1952).

2 *Id*. at 188.

3 *Id*. at 190

4 *Id*. at 191.

5 *Id*. at 195 (Franfurter, J., concurring).

6 Frederick Schauer, *Fear, Risk and the First Amendment: Unraveling the Chilling Effect*, 58 B.U. L. REV. 685, 685 (1978); *see also* Baird v. State Bar of Arizona, 401 U.S. 1 (1971); Keyishian v. Board of Regents, 385 U.S. 589 (1967); Lamont v. Postmaster General, 381 U.S. 301 (1965); Baggett v. Bullitt, 377 U.S. 360 (1964).

7 U.S. CONST. amend. I, which protects freedom of speech and expression, and states: "Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances."

8 Laird v. Tatum, 408 U.S. 1, 4-5 (1972). For additional discussion of *Laird*, see Anjali S. Dalal, *Shadow Administrative Constitutionalism and the Creation of Surveillance Culture*, 2014 MICH. ST. L. REV. 61 (2014).

9 Comment, Laird v. Tatum: *The Supreme Court and a First Amendment Challenge to Military Surveillance of Lawful Civilian Political Activity*, 1 HOFSTRA L. REV. 244 (1973); *see also Laird*, 408 U.S. at 6.

10 *Id*.

11 Jonathan R. Siegel, Note, *Chilling Injuries as Basis for Standing*, 98 Yale. L. J. 905, 906 (1989).

12 *Laird*, 408 U.S. at 9.

13 *Id*. at 13-14.

14 *Id*. at 10.

15 380 U.S. 479 (1965)

16 *Id*. at 486.

17 *Id*. at 487.

18 493 F.3d 644, 648 (6th Cir. 2007) (internal quotation marks and citations omitted).

19 *Id*. at 653 (emphasis added).

20 *Id*. at 661 (internal quotation marks and citations omitted).

21 *Id*.

22 Pub. L. No. 110–261, 122 Stat. 2436.

23 133 S. Ct. 1138, 1145 (2013).

24 *Id*. at 2.

25 673 F. 3d 902, 906 (9th Cir. 2011).

26 *Id*. at 912 (internal quotation marks omitted).

27 *Id*. at 913 (internal quotation marks omitted).

28 *See generally,* Dalal, *supra* note 8.

29 *Id.* (citing N.Y. Times Co. v. U.S. Dep't of Justice, No. 11 Civ. 9336, 2013 WL 50209, at *1 (S.D.N.Y. Jan. 2, 2013))

30 For a deeper study of the Attorney General Guidelines, see Dalal, *supra* note 8.

31 *Id.*; *see also* OFFICE OF THE ATTORNEY GENERAL, U.S. DEP'T OF JUSTICE, THE ATTORNEY GENERAL'S GUIDELINES ON GENERAL CRIMES, RACKETEERING ENTERPRISE, AND TERRORISM ENTERPRISE INVESTIGATION § VI(A)(2) (2002), *available at* https://www.fas.org/irp/agency/doj/fbi/generalcrimes2.pdf [hereinafter ASHCROFT GUIDELINES].

32 *Id.*

33 *Id.*; *see also* ASHCROFT GUIDELINES, § VI(A).

34 *Id.*; *see also* Press Release, Department of Justice, Fact Sheet: Attorney General Consolidated Guidelines for FBI Domestic Operations § II(A) (Oct. 3, 2008), http://www.justice.gov/opa/pr/2008/October/08-ag-889.html [hereinafter Mukasey Guidelines]

35 Mukasey Guidelines, supra note 35, § II(A).

36 Ibrahim v. Department of Homeland Sec., 669 F.3d 983, 989 (9th Cir. 2012).

37 *Id.*

38 Adam Goldman & Matt Apuzzo, *With CIA Help, NYPD Moves Covertly in Muslim Areas*, ASSOCIATED PRESS (Aug. 23, 2011), *available at* http://www.ap.org/Content/AP-in-the-News/2011/With-CIA-help-NYPD-moves-covertly-in-Muslim-areas.

39 MUSLIM AMERICAN CIVIL LIBERTIES COALITION ET AL., MAPPING MUSLIMS: NYPD SPYING AND ITS IMPACT ON AMERICAN MUSLIMS 10 (2013), http://www.law.cuny.edu/academics/clinics/immigration/clear/Mapping-Muslims.pdf [hereinafter MAPPING MUSLIMS].

40 *Id.* at 20.

41 Press Release, Office of the Mayor of New York City, Mayor Bloomberg, Police Commissioner Kelly and Microsoft Unveil New, State-Of-The-Art Law Enforcement Technology that Aggregates and Analyzes Existing Public Safety Data in Real Time to Provide a Comprehensive View Of Potential Threats and Criminal Activity (Aug. 8, 2012), http://www.nyc.gov/html/om/html/2012b/pr291-12.html.

42 *Id.*

43 *See* JOHN ROLLINS, CONG. RESEARCH SERV., RL34070, FUSION CENTERS: ISSUES AND OPTIONS FOR CONGRESS 1, (2008), *available at* http://fas.org/sgp/crs/intel/RL34070.pdf.

44 OFFICE OF JUSTICE PROGRAMS ET AL., FUSION CENTER GUIDELINES: DEVELOPING AND SHARING INFORMATION AND INTELLIGENCE IN A NEW ERA 2 (2006), *available at* http://it.ojp.gov/documents/fusion_center_guidelines_law_enforcement.pdf.

45 ROLLINS, *supra* note 43, at 34.

46 *Id.* at 2.

47 *Id.* at 15-17.

48 MAPPING MUSLIMS, *supra* note 39, at 12.

49 *Id.* at 14.

50 *Id.* at 18.

51 *Id.*

52 *Id*. at 22.

53 *Id*.

54 *Laird*, 408 U.S. at 21 (citing THE FEDERALIST NO. 41 (James Madison)).

55 Klayman v. Obama, 957 F. Supp. 2d 1 (D.D.C. 2013).

56 ACLU v. Clapper, 959 F. Supp. 2d 724 (S.D.N.Y. 2013).

57 Charlie Savage, *Federal Prosecutors, in a Policy Shift, Cite Warrantless Wiretaps as Evidence*, N.Y. TIMES, Oct. 26, 2013, at A21, *available at* http://www.nytimes.com/2013/10/27/us/federal-prosecutors-in-a-policy-shift-cite-warrantless-wiretaps-as-evidence.html?_r=0.

UNITED STATES OF AMERICA

USING COPYRIGHT LAW TO CENSOR SPEECH

Christina Mulligan

Perhaps more than any other nation, the United States prides itself as being a country where free speech reigns. Protections for speech are codified in the First Amendment to the US Constitution. "Congress shall make no law . . . abridging the freedom of speech, or of the press."[1] While the brevity of the speech and press clauses invites a variety of interpretations, the United States Supreme Court has consistently chosen a very speech-protective approach to First Amendment law. Laws prohibiting Nazi-sympathizers and racists from expressing themselves have been struck down.[2] Pornography, generally, is protected.[3] Religions can be denigrated by private citizens.[4] The American system of speech protection is sometimes considered so extreme that commentators in the European Union and other freedom-valuing states have criticized American jurisprudence as allowing far too much harmful speech to be made.[5]

Given the reputation of America's First Amendment, the notion that censorship may be a problem in the United States is unexpected. But there are several ways in which free expression is vulnerable in the United States, two of which will be explored here through the lens of copyright law. The first is through *automatic enforcement*, where flawed, automated systems remove or prevent communications without a human arbiter to

decide if the censorship is appropriate. The second is *the absence of procedural safeguards* in law enforcement regimes aimed at achieving otherwise reasonable ends. Where procedural safeguards are absent, a party can be censored without a meaningful opportunity to challenge the censorship, thereby allowing censors to abuse their role and to exert unchecked power.

It is worth noting that copyright law, strictly speaking, often has a censoring effect, even when the best of procedural safeguards are in place.[6] By its nature, it restricts who may use certain expressions to communicate. But this chapter isn't about the censoring effects of copyright law, per se. In fact, it assumes that some copyright laws, just as laws restricting underage pornography and speech that results in imminent, massive harm, may be in the public good even though they restrict certain acts of expression. What this chapter highlights is the fact that absent the right procedural and enforcement structures, laws that justifiably restrict one kind of speech can be abused to unjustifiably censor another.

COPYRIGHT AND THE FIRST AMENDMENT

Although American jurisprudence is highly protective of speech, there are certain kinds of laws regulating speech which are legally permitted. Some of these laws regulate what is considered "low value" speech, such as libel or insulting, "fighting" words.[7] But copyright laws, despite restricting the transmission of what is often very valuable or important speech, are also permitted because they were plainly contemplated in Article 1, Section 8, of the United States Constitution.[8] When adopted, the Constitution specified that Congress would have the power to "promote the Progress of Science and useful Arts, by securing for limited Times to Authors and Inventors the exclusive Right to their respective Writings and Discoveries."[9] Although the First Amendment was adopted shortly thereafter, the United States Supreme Court has ruled that, as a general matter, the First Amendment does not meaningfully limit Congress' ability to legislate copyright laws.[10] Many scholars have criticized two of the Supreme Court's recent decisions, *Eldred v. Ashcroft* and *Golan v. Holder*, for giving Congress too much power to increase the duration and breadth of copyright protection.[11] But regardless of whether the ultimate conclusions of *Eldred* and *Golan* were wise, the Court's reasoning was deeply problematic

because it failed to recognize the real and potential censoring effects of America's copyright law on non-copyright-infringing speech.

NOTICE-AND-TAKEDOWN

One portion of copyright law that opens the door to censorship of non-copyright-infringing speech is the notice-and-takedown system created by the Digital Millennium Copyright Act ("DMCA"). Prior to the DMCA, a service such as YouTube risked overwhelming liability for hosting, and necessarily reproducing, a user's copyright-infringing content,[12] while being unable to prevent that copyright infringement because of the scale of its operations.[13] The notice-and-takedown regime implemented by the DMCA acts to protect online service providers from this liability, granting them immunity from copyright infringement so long as they remove allegedly-infringing content upon receipt of "notice" from a purported copyright owner or its agent.[14] Although the notice must contain a "statement that the complaining party has a good faith belief that use of the material . . . is not authorized," it need not include any evidence or reasoning.[15] Upon receipt of a takedown notice, hosts of digital content must then take down the content and inform the uploading user that someone has claimed that the user's content is copyright infringing. The user then has the opportunity to send a "counter notice," claiming that the content is not infringing.[16] If the user sends a counter notice, an online service provider must restore the content within 10 to 14 days.[17] After receiving the counter-notice, the copyright owner must bring a lawsuit against the uploader to have the content removed. Even if the content is infringing, an online service provider won't be liable for leaving it up.[18]

At first impression, notice-and-takedown seems like a good idea. It gives copyright owners an easy and inexpensive way to get infringing content removed from the Internet, and it provides legal immunity to useful, value-creating businesses in return for complying with copyright owners' notices. Without this "safe harbour" afforded to online service providers, YouTube would not exist as we know it.

Nonetheless, the notice-and-takedown system also opens the door to censoring non-copyright-infringing material. When someone files a notice naming a piece of content, a host must take down the content in order to retain immunity from a copyright lawsuit. As a result, hosts have every

incentive to take down everything they receive a notice about — even when the notice is frivolous. This incentive is only increased when a host's operations are large enough that staff would be overwhelmed by the task of trying to analyze the reasonableness of individual notices. As a result, bogus notices can and do get sent. Although notice-givers can theoretically face liability for knowingly misrepresenting that content is copyright infringing,[19] in practice these suits are rare and the "knowingly" standard is difficult to meet.[20] As a result, there is very little motivation for a person not to send a takedown notice for content he simply does not like.

Bogus notices can and have had censoring effects on substantive, political speech, notably in the past two US presidential elections.[21] In 2008, the John McCain campaign used several news clips in its ads, which were removed from YouTube when takedown notices were sent by CBS, Fox, NBC, and the Christian Broadcasting Network.[22] Even after receiving a counter notice from the McCain campaign claiming fair use, YouTube was required to keep the video down for a minimum of 10 days to retain its immunity from suit.[23] So when the McCain campaign pleaded with YouTube to restore the video sooner, YouTube responded in a detailed letter, explaining that "[b]ecause of the DMCA's structure, an abusive takedown notice may result in the restriction of non-infringing speech during the statutory 10-day waiting period. . . . [A] detailed substantive review of every DMCA notice is simply not possible due to the scale of YouTube's operations. . . . No number of lawyers could possibly determine with a reasonable level of certainty whether all the videos for which we receive disputed takedown notices qualify as fair use."[24] The letter explained that restoring the McCain campaign's ad early, while not investigating other potential abuses, simply would not be fair.[25] "We try to be careful not to favor one category of content on our site over others, and to treat all of our users fairly, regardless of whether they are an individual, a large corporation or a candidate for public office."[26]

Four years later, YouTube responded to a similar incident differently. In mid-July of 2012, Mitt Romney put a campaign ad on YouTube, criticizing President Barack Obama's relationship with campaign donors.[27] The ad juxtaposed a clip of Obama singing one line from Al Green's song, "Let's Stay Together", with news headlines describing Obama's rewarding of campaign donors and lobbyists.[28] The "Let's Stay Together" music pub-

lisher, BMG, issued a takedown notice for the video, and it was removed.[29] The takedown appeared to be politically motivated because many copies of original videos of Obama singing the song at first remained visible.[30] But, as blogger Mike Masnick pointed out, "[i]t appears that someone pointed out to BMG's lawyers that *this looks really bad*," and takedowns were issued to the original videos as well.[31] Just two days later, following significant criticism in the media, YouTube restored all of the videos,[32] despite the fact that it would lose legal immunity if it did not keep the videos down for at least 10 days following the Romney campaign's counter notice.

While one's first instinct may be to feel frustration that the Romney campaign got preferential treatment compared to the average YouTube uploader, it is perhaps more important to be frustrated that YouTube cannot routinely ignore meritless takedown notices. Faced with bad publicity, YouTube deviated from its standard practice because holding to it visibly flew against the free speech values so central to the American political process. The problem is not so much that the Romney campaign ad got YouTube's attention, but that the existing system makes it effectively impossible for all other meritless notices to be ignored.

Admittedly, the effect of takedown notices is tolerable for many legally sophisticated uploaders — if they file a counter-notice, content will only stay down for 10 to 14 days and then be restored.[33] But YouTube users without legal training or who don't have much experience uploading may choose not to file a counter-notice out of a misplaced fear that they have done something wrong. Those individuals' speech will remain censored as a result.

Other aspects of the notice-and-takedown system have a plainly censoring effect that speakers have little ability to counteract, specifically the process for issuing a notice to remove a link that leads to allegedly infringing material. When a copyright owner notifies Google or Bing that one of the search engine's links leads to copyright-infringing content, the search engine must delete the link from its search results to maintain immunity from a copyright lawsuit,[34] but does not have to (and often does not have a convenient means to) inform the website owner or author that the link has been removed.[35] Even if the website owner discovers the takedown was issued and disagrees, there is no counter-notification procedure that allows a search engine to restore the link and maintain immunity.

The lack of procedural safeguards to prevent meritless notices from being acted on has resulted in important, political speech being obscured from public view. For example, in late 2011, when the public was debating the proposed Stop Online Piracy Act (SOPA), blogger Michael Masnick wrote a post about why SOPA should not be passed. He later discovered that the post had been removed from Google's search results.[36] The "anti-piracy" firm Armovore, on behalf of a pornography company, Paper Street Cash, had sent a notice to Google, asking for it to remove the link to Masnick's webpage, supposedly because the page was infringing Paper Street Cash's copyrights.[37] There was nothing even arguably infringing in the post or user comments, and Google eventually put the blog post back in its search index.[38] After Masnick wrote about the takedown, Armovore reached out to "'accept full responsibility for the mistake' and insist that while that takedown was an automated keyword-based effort, they now only do manual takedowns."[39]

More recently, movie studios Viacom, Paramount, Fox, and Lionsgate used notice-and-takedown to remove the Google search engine's links to a documentary[40] about the file-sharing website, The Pirate Bay, by film director Simon Klose.[41] It's possible the studios acted maliciously because of the film's sympathetic depiction of file-sharers, or that the studios' automatic systems which send takedown notices made several completely unjustified mistakes. Either way, copies of the film became harder to locate and access. Klose responded in a video directed towards the film studios. "So regardless of whether you guys are trying to censor me actively, intentionally, or if your censoring technology just basically sucks, the result is the same. You are hurting my distribution strategy. To me, this becomes a question of freedom of speech. You guys are silencing my story."[42]

Takedown notices can and have become a tool for censorship because the regime allows for pretextual notices to be sent by private parties, without any showing that the alleged work is copyrighted or owned by the notice-giving party. When links to a work are removed, the aggrieved party has nearly no recourse against the notice-filer and no formal procedure to get the links restored. When content is removed, filing a counter-notice will eventually restore the content; however, the counter-notification protection is cold comfort to one worried about censorship, especially when the protection can be removed or weakened by the legislature.

AUTOMATED INFRINGEMENT DETECTION SYSTEMS

In other circumstances, hosting services are voluntarily partnering with copyright holders to automatically remove infringing content without notices being filed. The choices of what to remove are made by an algorithm, not by humans, and so content which should never be censored often is. In 2012, Michelle Obama's speech at the Democratic National Convention was mistakenly blocked on YouTube shortly after it concluded.[43] Just the day before, the live stream of the Hugo Awards was cut off by bots who flagged the ceremony's clips of Dr. Who episodes as copyright infringing — even though the clips were used with permission and had been provided to the awards by the studio.[44] One of NASA's official clips from the 2012 Mars landing was also accidentally flagged by YouTube's Content ID system that registered it as belonging to a news station that had broadcast the clip earlier.[45]

Although Content ID systems are not required by law and don't provide any greater legal benefit to online service providers than complying with the DMCA, service providers are increasingly employing them out of fear that failure to go "above and beyond" the requirements of the law will result in hassles from content providers and lobbying to eliminate the safe harbours and other protections afforded to online service providers under the DMCA.[46]

DOMAIN NAME SEIZURES

A recent bout of domain name seizures provides another example of how non-infringing speech can be censored in the name of copyright law. Under the authority of the Pro-IP Act, the Immigration and Customs Enforcement (ICE) arm of the Department of Homeland Security began a series of domain name seizures in June 2010,[47] with the goal of "seiz[ing] the domain names of websites that were selling counterfeit goods and providing access to infringing content."[48] While many would support these twin goals, once again, the lack of a meaningful opportunity to challenge the seizures led to censorship of content in cases where no counterfeiting or copyright infringement was occurring. In one instance, a seizure resulted in 84,000 innocent subdomains being seized, most of which were personal or small business websites.[49] The seizures did not take the content on the sites, but rather changed what users would see when they typed the do-

main name into their browsers. Instead of the site they were familiar with, they would see a notice that the site had been seized by ICE.

One of the most offensive seizures was of a hip-hop blog, dajaz1.com. Dajaz1.com was alleged to be a "linking site" — a site that provided links to infringing content hosted elsewhere. The blog was hardly a site dedicated to promoting copyright infringement. In fact, some pre-release content linked on dajaz1.com had been sent to the website owners by record companies, in order to promote the new music.[50] The owner of dajaz1.com was soon embroiled in a procedural nightmare to get their domain name returned. Despite retaining sophisticated counsel, the domain was not returned for over a year, after a Kafkaesque runaround.[51] Because the owner of dajaz1.com requested the return of the domain, the government had to either return the domain name or begin a full, adversarial forfeiture process. However, the deadline came and went without the domain name being returned or a forfeiture procedure beginning. The government claimed they had been granted an extension of time to begin the forfeiture, but refused to show the order to dajaz1.com's lawyer, Andrew Bridges, because it had been filed under seal. Bridges pressed for the opportunity to oppose further extensions and was denied; when Bridges asked for proof that the government had actually filed and received the extensions, the US attorney said Bridges would just have to trust him. Eventually the government decided not to file for forfeiture, and the dajaz1.com domain was returned to its owners, over a year after it was seized.

Five months after the domain name was returned, further legal efforts resulted in the court filings concerning dajaz1.com being unsealed. The requests for extensions of time to file for forfeiture were made because the government was waiting for evidence from the Recording Industry Association of America (RIAA) in order to build its case.[52] Electronic Frontier Foundation legal director Cindy Cohn characterized the injustice — "Here you have ICE making a seizure, based on the say-so of the record company guys, and getting secret extensions as they wait for their masters, the record companies, for evidence to prosecute. This is the RIAA controlling a government investigation and holding it up for a year."[53]

AVOIDING CENSORSHIP IN THE FUTURE

As one commenter observed after the dajazı.com fiasco, if the government had seized a magazine printing press instead of a domain name, the public would likely have been up in arms.[54] But the cover of copyright law enforcement lulls the public into a false sense that the seizures must be justified, because it believes that preventing copyright infringement in general is often justified. But the term "copyright" — as well as "terrorism" and "child pornography" — cannot be a shibboleth which, when uttered, gives the government and private actors unrestricted power to censor legal speech without recourse. Rather, we should all be wary of any law that restricts speech even when it superficially appears to be in the public good, and always consider how the law can be abused before throwing support behind it.

1 U.S. CONST. amend. I.

2 *See, e.g.*, Virginia v. Black, 538 U.S. 343 (2003); R.A.V. v. City of St. Paul, 505 U.S. 377 (1992); National Socialist Party of America v. Village of Skokie, 432 U.S. 43 (1977).

3 Pornography may only be banned under United States law if "the average person, applying contemporary community standards would find that the work, taken as a whole, appeals to the prurient interest, . . . the work depicts or describes, in a patently offensive way, sexual conduct specifically defined by the applicable state law[, and] . . . the work, taken as a whole, lacks serious literary, artistic, political, or scientific value." Miller v. California, 413 U.S. 15 (1973).

4 *See* Cantwell v. Connecticut, 310 U.S. 296 (1940).

5 *See, e.g.,* Sionaioh Douglas-Scott, T*he Hatefulness of Protected Speech: A Comparison of the American and European Approaches*, 7 WM. & MARY BILL RTS. J. 305 (1999); Michel Rosenfeld, *Hate Speech in Constitutional Jurisprudence: A Comparative Analysis*, 24 CARDOZO L. REV. 1523 (2003); Guy E. Carmi, *Dignity Versus Liberty: The Two Western Cultures of Free Speech*, 26 B.U. INT'L L.J. 277 (2008).

6 *See generall*, Rebecca Tushnet, *Copy This Essay: How Fair Use Doctrine Harms Free Speech and How Copying Serves It*, 114 YALE L.J. 535 (2004).

7 *See* Chaplinsky v. State of New Hampshire, 315 U.S. 568, 572 (1942).

8 *See* Eldred v. Ashcroft, 537 U.S. 186, 219 (2003) ("The Copyright Clause and First Amendment were adopted close in time. This proximity indicates that, in the Framers' view, copyright's limited monopolies are compatible with free speech principles.").

9 U.S. CONST. art. 1, § 8.

10 *See Eldred*, 537 U.S. at 219-221; Golan v. Holder, 132 S.Ct. 873, 889-94 (2012).

11 *See, e.g.*, Lawrence Lessig, *After the Battle Against SOPA-What's Next?*, THE NATION, Jan. 18, 2012, http://www.thenation.com/article/165901/after-battle-against-sopa-whats-next; Gerard Magliocca, *Empty Formalism in Golan and Eldred*, CONCURRING OPINIONS, Jan. 18, 2012, http://www.concurringopinions.com/archives/2012/01/empty-formalism-in-golan-and-eldred.html; Jason Mazzone, *Golan/SOPA*, BALKINIZATION, Jan. 18, 2012, http://balkin.blogspot.com/2012/01/golansopa.html; Wendy Seltzer, *Copyright in Congress, Court, and Public*, http://wendy.seltzer.org/blog/archives/2012/01/19/copyright-in-congress-court-and-public.html (Jan. 19, 2012). In Eldred, the Court upheld Congress's decision to extend the copyright term for twenty extra years, and in Golan, the Court allowed Congress to retroactively grant copyright protections to works already in the public domain. S*ee Eldred*, 537 U.S. 186; *Golan*, 132 S.Ct. 873.

12 The controversial history surrounding why accessing digital content is often considered a reproduction of a copyrighted work is described in greater detail in Christina Mulligan, *Technological Intermediaries and Freedom of the Press*, 66 S.M.U. L. REV. 157 (2013), *available at* http://ssrn.com/abstract=2224058.

13 For example, approximately a hundred hours of footage is uploaded to YouTube every minute. Statistics, YouTube.com, http://www.youtube.com/yt/press/statistics.html (last visited July 27, 2013).

14 *See* 17 U.S.C. § 512(c).

15 17 U.S.C. § 512(c)(3)(A)(v).

16 17 U.S.C. § 512(g)(2).

17 *Id*.

18 *See* 17 U.S.C. § 512(g)(4).

19 17 U.S.C. § 512(f).

20 Wendy Seltzer, *Free Speech Unmoored in Copyright's Safe Harbor: Chilling Effects on the DMCA on the First Amendment*, 24 HARV. J.L. & TECH. 171, 221-25 (2010).

21 The McCain, Romney, and Techdirt takedown notices are also described in Mulligan, *supra* note 12.

22 17 U.S.C. § 512(g)(2)(C); Seltzer, *supra* note 20, at 172.

23 Seltzer, *supra* note 20, at 172-73.

24 Letter from Zahavah Levine, Chief Counsel, YouTube, to Trevor Potter, Gen. Counsel, McCain-Palin 2008, at 1–2 (Oct. 14, 2008), *available at* http://wendy.seltzer.org/media/youtube-letter-20081014.pdf.

25 *Id*. at 2-3.

26 *Id*.

27 *See* mittromney, *Political Payoffs and Middle Class Layoffs*, YOUTUBE (July 16, 2012), http://www.youtube.com/watch?v=GIajeW6xPnI.

28 *Id*.; Timothy B. Lee, *Music Publisher Uses DMCA to Take Down Romney Ad of Obama Crooning*, ARS TECHNICA, July 16, 2012, http://arstechnica.com/tech-policy/2012/07/major-label-uses-dmca-to-take-down-romney-ad-of-obama-crooning/.

29 Lee, *supra* note 28.

30 Mike Masnick, *Even Obama Is a Pirate: BMG Issues New Takedown on Original Obama Singing Al Green Clip*, TECHDIRT, July 17, 2012, http://www.techdirt.com/articles/20120717/13500819733/bmg-doubles-down-issues-takedown-original-clip-obama-singing-al-green.shtml.

31 *Id*.

32 Steve Friess, *YouTube Restores Romney's Ad Despite Rights Claim*, POLITICO (July 19, 2012), http://www.politico.com/news/stories/0712/78739.html.

33 *See* 17 U.S.C. § 512(g)(2)(C).

34 17 U.S.C. § 512(d).

35 *See* 17 U.S.C. § 512(g) (specifying restoration and counter-notification procedures for material stored with a service provider, but not for material discoverable through information-location tools).

36 Mike Masnick, *Key Techdirt SOPA/PIPA Post Censored by Bogus DMCA Takedown Notice*, TECHDIRT (Feb. 27, 2012), http://www.techdirt.com/articles/20120223/15102217856/key-techdirt-sopapipa-post-censored-bogus-dmca-takedown-notice.shtml.

37 *Id*.

38 Mike Masnick, *Company That Issued Bogus Takedown Notice Says It Was All a Mistake, Apologizes*, TECHDIRT (Feb. 28, 2012), http://www.techdirt.com/articles/20120228/09424117897/com-

pany-that-issued-bogus-take-down-says-it-was-all-mistake-apologizes.shtml.

39 *Id*.

40 *See* THE PIRATE BAY: AWAY FROM KEYBOARD, http://watch.tpbafk.tv/ (last visited July 27, 2013).

41 Mike Masnick, *Major Hollywood Studios All Sent Bogus DMCA Takedowns Concerning The Pirate Bay Documentary*, TECHDIRT, May 20, 2013, http://www.techdirt.com/articles/20130520/11552823150/major-hollywood-studios-all-sent-bogus-dmca-takedowns-concerning-pirate-bay-documentary.shtml.

42 Simon Klose, *An Open Letter to Hollywood Studios Censoring TPB AFK*, THE PIRATE BAY - AWAY FROM KEYBOARD (May 22, 2013), http://www.tpbafk.tv/2013/05/an-open-censoring-tpb-afk.

43 Ryan Singel, *YouTube Flags Democrats' Convention Video on Copyright Gounds*, WIRED (Sept. 5, 2012), http://www.wired.com/threatlevel/2012/09/youtube-flags-democrats-convention-video-on-copyright-grounds/.

44 Zachary Knight, *Copyright Enforcement Bots Seek and Destroy Huge Awards*, TECHDIRT (Sept. 5, 2012), http://www.techdirt.com/articles/20120903/18505820259/copyright-enforcement-bots-seek-destroy-hugo-awards.shtml.

45 Parker Higgins, *Mars Landing Videos, and Other Casualties of the Robot Wars*, EFF DEEPLINKS BLOG (Aug. 8, 2012), https://www.eff.org/deeplinks/2012/08/mars-landing-videos-and-other-casualties-robot-wars.

46 Content ID systems also allow rightsholders to monetize use of their works easily, by partnering with online service providers to place advertisements or links to paid downloads near infringing content rather than having it taken down, as in the examples above. S*ee How Content ID Works*, YOUTUBE HELP, https://support.google.com/youtube/answer/2797370 (last visited July 28, 2013).

47 For a substantially more detailed account of the domain name seizures, see ANDY SELLARS, SEIZED SITES: THE *IN REM* FORFEITURE OF COPYRIGHT INFRINGING DOMAIN NAMES 3–15 (May 8, 2011), http://ssrn.com/abstract=1835604.

48 U.S. INTELLECTUAL PROPERTY ENFORCEMENT COORDINATOR, 2010 U.S. INTELLECTUAL PROPERTY ENFORCEMENT COORDINATOR ANNUAL REPORT ON INTELLECTUAL PROPERTY ENFORCEMENT 6 (2011), *available at* http://www.whitehouse.gov/sites/default/files/omb/IPEC/ipec_annual_report_feb2011.pdf.

49 *See, e.g.,* Nate Anderson, *Silicon Valley Congresswoman: Web Seizures Trample Due Process (and Break the Law)*, ARS TECHNICA (Mar. 14, 2011), http://arstechnica.com/tech-policy/2011/03/ars-interviews-rep-zoe-lofgren/; Ernesto Van Der Sar, *U.S. Government Shuts Down 84,000 Websites*, TORRENTFREAK (Feb. 16, 2011), http://torrentfreak.com/u-s-government-shuts-down-84000-websites-by-mistake-110216/.

50 Ben Sisario, *Music Web Sites Dispute Legality of Their Closing*, N.Y. TIMES, Dec. 19, 2010, at B6, *available at* http://www.nytimes.com/2010/12/20/business/media/20music.html.

51 Mike Masnick, *Breaking News: Feds Falsely Censor Popular Blog For Over a Year, Deny All Due Process, Hide All Details...*, TECHDIRT (Dec. 8, 2011), http://www.techdirt.com/articles/20111208/08225217010/breaking-news-feds-falsely-censor-popular-blog-over-year-deny-all-due-process-

hide-all-details.shtml.

52 David Kravets, *Feds Seized Hip-Hop Site for a Year, Waiting for Proof of Infringement*, WIRED (May 3, 2013), http://www.wired.com/2012/05/weak-evidence-seizure/.

53 *Id*.

54 Masnick, *supra* note 51.

SOUTH AFRICA & ZIMBABWE

SILENCING CRITICAL VOICES

Caroline B. Ncube & Eve Gray

INTRODUCTION

In general, the situation in both South Africa and Zimbabwe is very different from the 'Arab Spring' model, where mass uprisings used social media as advocacy and organizing tools followed by states switching off the internet or blocking access to it via mobile phones, as discussed in the chapter by Nagla Rizk. It is also quite different from the situation in China, were the target is public use of online media. In South Africa and Zimbabwe there are more incident-based instances of censorship, which pertain to specific media reports or information published online and to individual voices on social media platforms. Both countries have constitutional protection of freedom of expression, including press freedom. However, they both have legislation which has been used to secure the censorship of critical voices. It is not possible in a chapter of this length and type to engage in full-scale analysis of all relevant legislation. Therefore, the chapter only provides a snapshot of some of the relevant legislation. It aims to provide examples of the different types of censorship that have occurred in both countries in the last two years.

State information in South Africa is currently protected by the Protection of Information Act 84 of 1982. This Act will soon be repealed and replaced by the Protection of State Information Bill (B6D-2010), commonly known as the Secrecy Act. At the time of writing (November 2013) the

Secrecy Act has been passed by the Parliament but has been denied presidential assent due to constitutional concerns.[1] It is currently being reconsidered by an Ad Hoc Committee of Parliament. Access to information is regulated by the Promotion of Access to Information Act 2 of 2000 (hereinafter, 'PAIA'). The Electronic Communications and Transactions Act 25 of 2002 (hereinafter, 'ECTA'), which provides for internet service provider (ISP) liability, is also relevant to this discussion, and is the subject of another chapter in this book, written by Andrew Rens. Censorship is often closely linked to surveillance and interception of communications. South Africa's Regulation of the Interception of Communications Act 70 of 2002 (hereinafter, 'RICA') is also directly relevant. It is not discussed in this chapter and readers are referred to other writings on the topic.[2] This chapter will only focus on the provisions of the Secrecy Act.

State information in Zimbabwe is protected by the Official Secrets Act,[3] and access to non-state information is regulated by the Access to Information and Protection of Privacy Act.[4] Like South Africa, Zimbabwe has legislation regulating the interception of communication, namely the Interception of Communications Act.[5] In addition, Zimbabwe's Public Order and Security Act[6] creates the criminal offence of insulting the president.[7] Similarly, the Criminal Law (Codification and Reform) Act,[8] creates the offence of undermining or insulting the President. Zimbabwe has a new Constitution, adopted in the first quarter of 2013. This will necessitate the evaluation and amendment of all of the above legislation to ensure that it complies with the new Constitution. As will be shown below, some of these provisions have already been struck down by the Constitutional Court.

SOUTH AFRICA

Section 16 of South Africa's Constitution provides for the freedom of expression, which expressly includes 'the freedom of the press and other media'.[9] It also lists the 'right to receive or impart information or ideas'. Section 32 provides for the right to access state information as follows:

(1) Everyone has the right of access to —

(a) any information held by the state, and;

(b) any information that is held by another person and that is required for the exercise or protection of any rights;

(2) National legislation must be enacted to give effect to this right, and may provide for reasonable measures to alleviate the administrative and financial burden on the state.

These constitutional provisions have been further fleshed out by PAIA and its regulations over which the South African Human Rights Commission (SAHRC) has been given oversight. The SAHRC's main role relates to monitoring the implementation of the Act and reporting on this annually to Parliament. Whilst the legislation has been implemented to some extent, it has been pointed out that it has not been as successful as expected mainly due to limited public knowledge of the legislation which means that only a few requests for information have been filed.

South African media has used these provisions to obtain information on which they have reported, particularly in relation to state corruption, to the chagrin of the state. In other instances, information forming the basis of such media reports has been provided by whistleblowers who work for, or with, the state. The state's response has been varied. This chapter focuses on its arguments that some of this information ought not to be disclosed as to do so would be detrimental to national security.

Like its predecessor, the Secrecy Act will allow the state to cordon off certain information on the basis of state security. The media and other stakeholders pushed back against the passage of the Secrecy Act arguing that it is nothing but an attempt to hide wrongdoing under the pretext of security concerns.[10] The initial lack of any protection for whistleblowers was considered as a deliberate ploy to discourage whistleblowing. Other arguments centred on the harshness of the penalties prescribed for convictions on the offences created by the Act. Despite such contestation, the (revised) Secrecy Act was passed by Parliament on 25 April 2013. As noted above, the President declined to sign the bill and referred it back to Parliament in September 2013. Under the Secrecy Act, certain state organs will be able to classify certain information as sensitive and thus put it beyond the reach of the media and any subsequent public scrutiny.

It is against this background that we consider the role of the Internet and how the tensions between press freedom and the protection of state information are likely to be played out. The major concern here is that, under the new regulatory regime created by the Secrecy Act, the media

will be unable to report on significant issues. This is because their possession of relevant information,[11] their failure to surrender this information to the relevant authorities[12] and any unlawful an intentional disclosure or publication of this information will constitute criminal offences.[13] Section 41 provides for a public interest defence in the following terms:

> *Any person who unlawfully and intentionally discloses or is in possession of classified state information in contravention of this Act is guilty of an offence and is liable to a fine or imprisonment for a period not exceeding five years, except where such disclosure or possession—*
>
> *(a) is protected or authorised under the Protected Disclosures Act, 2000 (Act No. 26 of 2000), the Companies Act, 2008 (Act No. 71 of 2008), the Prevention and Combating of Corrupt Activities Act, 2004 (Act No. 12 of 2004), the National Environmental Management Act, 1998 (Act No. 107 of 1998), or the Labour Relations Act, 1995 (Act No. 66 of 1995);*
>
> *(b) is authorised in terms of this Act or any other Act of Parliament; or*
>
> *(c) reveals criminal activity, including any criminal activity in terms of section 45 of this Act.*

A few observations about this section are necessary. First, it is a revised version of the defence that was provided for in earlier versions of the Secrecy Bill, namely clause 43 of the Protection of State Information Bill 6B of 2010/2011. Clause 43 of Bill B6B read as follows:

> Any person who unlawfully and intentionally discloses classified information in contravention of this Act is guilty of an offence and liable to a fine or imprisonment for a period not exceeding five years, except where such disclosure is —
>
> *(a) protected under the Protected Disclosures Act, 2000 (Act No. 26 of 2000) or section 159 of the Companies Act, 2008 (Act No. 71 of 2008); or*
> *(b) authorised by any other law.*

Clause 43 was clearly narrower than the current s41 as it contained a shorter list of legislation in paragraph (a) and did not contain paragraph (c). It was criticized for not incorporating a full public interest defence.[14] Secondly, section 41 of the Secrecy Act contains limited whistleblower protection but does not provide for a full public interest defence as had been called for by numerous stakeholders.[15] The defence is not a full defence as it is limited to disclosures about criminal activity only. It does not extend to improper conduct such as compromised tender processes.

Thirdly, reliance on the section 41 defence requires that the person disclosing information must first ascertain that the information he wants to report or disclose is protected by the specified legislation or actually relates to the commission of a criminal offence. This necessitates reliance upon legal advice. The process of obtaining such advice may take some time and thus delay the disclosure of certain information. In some cases this may be detrimental to the public interest as the allegedly criminal activities will continue in the interim.

South Africa has had its fair share of conflicts in relation to access to information. One of the most well-known conflicts relates to the Arms Deal scandal that has been under public scrutiny since it was signed in 1999. One of the key players in the matter, Richard Young, Managing Director of CCII Systems (Proprietary) Ltd. successfully applied to the High Court for state information to support his claims that CCII's bid to supply information management to support the Arms Deal.[16] The fact that the state refused to give Young information on the basis of sensitivity until he obtained a High Court order may be seen as an example of the state withholding information.

Another well-known case is that of Project Avani in which hoax e-mails were allegedly sent by the National Intelligence Agency (NIA) to discredit some contestants in the presidential race.[17] Another controversial issue that has been the subject of media scrutiny is the upgrades to the president's rural homestead in Nkandla, KwaZulu-Natal. Being a presidential residence, this property is protected by the National Key Points Act 102 of 1980 and the disclosure of certain information about it, may be an offence.[18] It has been argued that had these events occurred after the enactment of the Secrecy Act, the media would not have been able to report on them without attracting criminal liability as they could have been classified.[19] These matters were ultimately reported in the print media and the newspapers' websites or electronic editions. Therefore any attempts to censor the contents of print media inevitably extends to the internet as well.

Old school state censorship was evident in the arrest of a Sunday Times Journalist, Mzilikazi wa Africa in 2010. Whilst not expressly stated as the reason for his arrest, the arrest appears to have been linked to his reporting on alleged corrupt or criminal activities by the then Commissioner

of Police.[20] The relevant newspaper reports were published in the print edition of the Sunday Times, and also on the newspaper's website.

Another oft-cited incident of censorship is that of Brett Murray's 'Spear of the Nation' painting.[21] This painting was exhibited at the Goodman Gallery in Johannesburg in May 2013. It depicted the President of South Africa in a Leninist pose with his genitals exposed.[22] It was also published on the City Press newspaper's website. The exhibition and publication of the painting raised the issue of how to balance freedom of expression with the right to dignity, both of which are enshrined in the constitution. Was a demand to take down the picture an attempt to protect the President's dignity or an unjustified act of censorship?

A number of attempts were made to secure the removal from the painting from the Goodman Gallery. These included the instigation of a defamation claim by the President and negotiations with the gallery by the ruling party on behalf of the President. The Film and Publications Board classified the painting as pornography, which would have required its removal. However, this classification was later revoked. The picture was ultimately removed from the gallery after it was vandalized by two men on the same day. These men were arrested and, at the time of writing, are still being prosecuted for the crime of malicious damage to property.

The African National Congress, the President's political party, led a boycott of the City Press and demonstrations against the newspaper after it refused to remove the painting from its website. In the end, the editor of the newspaper apologized to the president's family and removed the picture from the newspaper's website.[23] However, by that time the painting had been posted on Wikipedia and other websites and had already gone viral.

A final example is the censorship of the First National Bank's (FNB's) 'You can help' online advertising campaign. FNB's campaign included statements by young South Africans criticizing the government was challenged as disrespectful political agitation by the ruling party and ultimately removed voluntarily from the bank's YouTube channel.[24] In neither of these incidents was there direct censorship by the state; in neither case did the state remove the material from the internet through litigation or prosecution. Rather, after robust national debates with strident voices on

both sides of the debate, FNB removed the videos from YouTube. However, this may be viewed as indirect state censorship in the sense that social pressure initiated primarily by the state ultimately led to self-censorship.

ZIMBABWE

In Zimbabwe threats of prosecution under various pieces of legislation have a chilling effect of freedom of expression and press freedom online. However, in March 2013 Zimbabwe adopted a new Constitution.[25] Section 61 of the Constitution, 2013 provides for freedom of expression and freedom of the media,[26] and section 62 provides for access to information.[27] These provisions are comprehensive and clear and should usher in a new era of freedom of expression, freedom of the media and access to state information. As noted above, Zimbabwe's existing legislation will have to be evaluated and amended if necessary to ensure compliance with these constitutional provisions.

Under the current legislative framework, there have been numerous reports of instances of old-school censorship. For example, within two years of the enactment of the Access to Information and Protection of Privacy Act (AIPPA), it was reported that there had been more than a dozen instances of arrest or other state harassment of journalists.[28] These incidents affected the print and online publication of certain stories.

Technical examination of the Internet infrastructure has shown that the state is not using any direct filtering of the Internet.[29] However, there have been reports of email surveillance, the use of an e-mail filtering system that blocks political content from reaching Reserve Bank employees and physical raids of Internet cafés where suspected illegal activity was taking place.[30] The suspected illegal activity was the dispatch of an email that was considered to be insulting to the President, which is criminalized by the Public Order and Security Act (POSA) and the Criminal Law (Codification and Reform) Act (CLCRA). However, on October 30, 2013, the Constitutional Court of Zimbabwe struck down sections 31(a)(iii) and 33(a)(ii) of the CLCRA which provided for the offences of 'publishing or communicating false statements prejudicial to the State' and 'undermining the authority of, or insulting, the President' respectively.[31]

In early June 2013, an individual began posting information about the allegedly corrupt activities of members of the ruling party in government on Facebook, under the pseudonym 'Baba Jukwa'.[32] This person claimed to be a disgruntled member of the ruling party who could no longer sit back and watch the wrongdoings in his party. He thus took to exposing them online. The ruling party's initial response was to shrug off Baba Jukwa, saying that he was entitled to his opinion and had the freedom to share it, if he so wished. This apparently noble stance was probably due to the fact that 2013 was an election year in Zimbabwe and it would not do for the ruling party to be seen to be aggressively censoring critical voices. However, appearances may be deceptive, and it seems that the police are trying to unmask Baba Jukwa,[33] and some online attackers have ostensibly locked the e-mail address that Baba Jukwa was using.[34] If these efforts are successful, he may be prosecuted.

CONCLUSION

Both countries have similar legislative frameworks that enable censorship to occur (see figure 1 below). The main difference is that Zimbabwe has legislation criminalizing insults to the President — whilst South Africa does not. However there have been calls for the introduction of such laws in South Africa.[35]

In both countries, there have been incidences of censorship of the press and individuals as recounted above. In many instances the information or views acted against are available in both print and online format. Action, though often primarily directed at the print or physical manifestation of the material, inevitably affects the Internet as well. All the instances outlined above have political overtones in that the newspaper or individual had expressed views that were considered to be critical of the sitting government. This then led not only to direct state censorship, but state-encouraged and censorship or the exertion of socio-political and economic pressure that led to the 'voluntary' removal of the material from the internet.

Aspect	South Africa	Zimbabwe
Classification of information	Protection of Information Act, 1982 to be repealed and replaced by the Protection of State Information Act, 2013; National Key Points Act, 1980.	Official Secrets Act, 1970.
Access to information	Promotion of Access to Information Act, 2000.	Access to Information and Protection of Privacy Act, 2002.
ISP liability	Electronic Communications and Transactions Act, 2002.	No specific statute.
Monitoring & interception of communications	Regulation of the Interception of Communications Act, 2002.	Interception of Communications Act, 2007.
Insult laws	No specific statute.	Public Order and Security Act, 2003; Criminal Law Codification and Reform Act [Chapter 9:23].

Figure 1: Relevant legislation in South Africa and Zimbabwe.

1 Parliamentary Monitoring Group, *Protection of State Information Bill: referral back by President* (Oct. 10, 2013), http://www.pmg.org.za/report/20131010-protection-state-information-bill-referral-back-president> (last visited Nov. 5, 2013).

2 Phillip De Wet and Alistair Fairweather *Spying far worse in South Africa than the U.S.*, MAIL AND GUARDIAN (June 13, 2013), http://mg.co.za/article/2013-06-14-00-spying-far-worse-in-south-africa. *See also*, Lauren Hutton, *Oh Big Brother, Where Art Thou? On the Internet, Of Course ... The Use of Intrusive Methods of Investigation by State Intelligence Services,* 16 AFRICAN SECURITY REV. 111, *and* Caroline B. Ncube, *Watching the Watcher: Recent Developments in Privacy Regulation and Cyber-Surveillance in South Africa,* (2006) 3 SCRIPT-ED 344, *available at* http://www.law.ed.ac.uk/ahrc/script-ed/vol3-4/ncube.asp.

3 Official Secrets Act of 1970, Chap. 11:09 (Zimbabwe).

4 Access to Information and Protection of Privacy Act of 2002, Chap. 10:27 (Zimbabwe). For a brief historical overview, see Caroline B. Ncube, *A Comparative Analysis of Zimbabwean and South African Data Protection Systems*, J. INFO. L. & TECH. (2004), http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2004_2/ncube/. For a detailed overview, see AFRICAN NETWORK OF CONSTITUTIONAL LAWYERS, NATIONAL STUDY ON ACCESS TO INFORMATION IN ZIMBABWE (2012), http://www.right2info.org/resources/publications/publications/national-study-on-access-to-information-in-zimbabwe-2012.

5 Chapter 20,

6 Public Order and Security Act of 2003, Chap. 11:17, s.16(2)(b) (Zimbabwe).

7 *See* Caroline B. Ncube, *The Dignity of the Office of the State President and the Freedom of Expression: Section 16(2)(b) of the Public Order and Security Act of 2003 (Zimbabwe),* 2004 TURF L. REV. 12 (2004).

8 Criminal Law (Codification and Reform) Act of 2004, Chap. 9:23 (Zimbabwe).

9 Section 16 provides:

> *(1) Everyone has the right to freedom of expression, which includes —*
> *(a) freedom of the press and other media;*
> *(b) freedom to receive or impart information or ideas;*
> *(c) freedom of artistic creativity; and*
> *(d) academic freedom and freedom of scientific research.*
> *(2) The right in subsection (1) does not extend to —*
> *(a) propaganda for war;*
> *(b) incitement of imminent violence; or*
> *(c) advocacy of hatred that is based on race, ethnicity, gender or religion, and that constitutes incitement to cause harm.*

10 *See* Secrecy Bill, RIGHT2KNOW CAMPAIGN, http://www.r2k.org.za/secrecy-bill (providing details of the campaign mounted by the Right2Know against the Secrecy Bill).

11 Section 41, Protection of State Information Bill, 2013.

12 Section 42.

13 Section 41.

14 *See* James Grant, *Defences under the Protection of State Information Bill: Justifications and the Demands of Certainty*, 28 SOUTH AFRICAN J. HUM. RTS. 328, 338 -339 (2012).

15 *See, e.g.*, R2K to protest Secrecy Bill vote, RIGHT2KNOW (Apr. 25, 2013), http://www.r2k.org.za/2013/04/25/secercy_bill_vote_protest.

16 *CCII Systems (Pty) Ltd v. Fakie NO* 2003 (2) SA 325 (T). There was a related Supreme Court of Appeal decision that did not affect the High Court's access to information ruling, *Fakie v CCII Systems (Pty) Ltd* [2006] SCA 54.

17 OFFICE OF THE INSPECTOR-GENERAL OF INTELLIGENCE, EXECUTIVE SUMMARY OF THE FINAL REPORT ON THE FINDINGS OF AN INVESTIGATION INTO THE LEGALITY OF THE SURVEILLANCE OPERATIONS CARRIED OUT BY THE NIA ON MR S MACOZOMA (2006), http://www.oigi.gov.za/Speeches/IG%20Exec%20Summary%2023%20Mar%2006.doc.

18 Pierre de Vos, *Nkandla: The Details Will, and Should, Be Made Public*, DAILY MAVERICK (May 16, 2013), http://www.dailymaverick.co.za/opinionista/2013-05-16-nkandla-the-details-will-and-should-be-made-public.

19 Ilham Rawoot, *Secrecy Bill: the Stories that Couldn't be Told*, MAIL & GUARDIAN (Sept. 9, 2011), http://mg.co.za/article/2011-09-09-secrecy-bill-the-stories-that-couldnt-be-told.

20 *See* Fienie Grobler, *Media Feedom under Spotlight as Reporter Arrested,* MAIL & GUARDIAN (Aug. 4, 2010), www.mg.co.za/article/2010-08-04-media-freedom-under-spotlight-as-reporter-arrested; *see also* Sapa, *Cops Admit Mzilikazi Wa Afrika Arrest Was Wrongful*, THE TIMES (Nov. 18, 2012), http://www.timeslive.co.za/local/2012/11/18/cops-admit-mzilikazi-wa-afrika-arrest-was-wrongful.

21 *See generally* David Freedberg, *Case of the Spear*, 11 ART SOUTH AFRICA 36 (Sept. 2012), *available at* http://www.columbia.edu/cu/arthistory/faculty/Freedberg/Case-of-the-Spear.pdf.

22 Matthew Burbidge, *Gallery Refuses to Remove "Spear of the Nation" Artwork*, MAIL & GUARDIAN (May 17, 2013), http://www.mg.co.za/2012-05-17-anc-irate-over-spear-of-the-nation-artwork.

23 Phillip de Wet, *Boycott Fails, but City Press Agrees to Drop "The Spear"*, MAIL & GUARDIAN (May 28, 2013), http://www.mg.co.za/article/2012-5-28-boycott-fails-but-city-press-agrees-to-drop-the-spear.

24 Sizwe same Yende, *FNB: Removal of Clips Doesn't Censor Young Voices*, CITY PRESS (Jan. 23, 2013), http://www.citypress.co.za/politics/fnb-removal-of-clips-doesnt-censor-young-voices.

25 CONST. OF ZIMBABWE, *available at* http://www.copac.org.zw.

26 Section 61 states:

> *1.Every person has the right to freedom of expression, which includes:*
>
> *a. freedom to seek, receive and communicate ideas and other information;*
>
> *b. freedom of artistic expression and scientific research and creativity; and*
>
> *c. academic freedom.*
>
> *2. Every person is entitled to freedom of the media, which freedom includes protection of the confidentiality of journalists' sources of information.*
>
> *3.Broadcasting and other electronic media of communication have freedom of establishment, subject only to State licensing procedures that:*
>
> *a. are necessary to regulate the airwaves and other forms of signal distribution; and*
>
> *b. are independent of control by government or by political or commercial interests.*
>
> *4. All State-owned media of communication must:*

a. be free to determine independently the editorial content of their broadcasts or other communications;

b. be impartial; and

c. afford fair opportunity for the presentation of divergent views and dissenting opinions.

5. Freedom of expression and freedom of the media exclude:

a. incitement to violence;

b. advocacy of hatred or hate speech; or

c. malicious injury to a person's reputation or dignity; or

d. malicious or unwarranted breach of a person's right to privacy.

27 Section 62 states:

1. Every Zimbabwean citizen or permanent resident, including juristic persons and the Zimbabwean media, has the right of access to any information held by the State or by any institution or agency of government at every level, in so far as the information is required in the interests of public accountability.

2. Every person, including the Zimbabwean media, has the right of access to any information held by any person, including the State, in so far as the information is required for the exercise or protection of a right.

3. Every person has a right to the correction of information, or the deletion of untrue, erroneous or misleading information, which is held by the State or any institution or agency of the government at any level, and which relates to that person.

4. Legislation must be enacted to give effect to this right, but may restrict access to information in the interests of defence, public security or professional confidentiality, to the extent that the restriction is fair, reasonable, necessary and justifiable in a democratic society based on openness, justice, human dignity, equality and freedom.

28 Article 19 & MISA-Zimbabwe, THE ACCESS TO INFORMATION AND PROTECTION OF PRIVACY ACT: TWO YEARS ON (2004), http://www.article19.org/data/files/pdfs/publications/zimbabwe-aippa-report.pdf.

29 OPENNET INITIATIVE, INTERNET FILTERING IN ZIMBABWE (2009), http://opennet.net/sites/opennet.net/files/ONI_Zimbabwe_2009.pdf

30 *Id.*

31 Zvamaida Murwira, *Concourt Strikes Down Sections of Statute Law,* THE HERALD (Oct. 31, 2013), http://www.herald.co.zw/concourt-strikes-down-sections-of-statute-law.

32 *See* Wikipedia, *Baba Jukwa*, http://en.wikipedia.org/wiki/Baba_Jukwa (as on Nov. 5, 2013).

33 Marry Anne Jolley, *Mugabe Offers $300,000 for Outing of Anonymous Whistleblower Baba Jukwa*, ABC NEWS (July 17, 2013), http://www.abc.net.au/news/2013-07-17/mugabe-offers-243002c000-for-outing-of-anonymous-whistleblower/4824498

34 Adam Taylor, *Has Baba Jukwa, Zimbabwe's Infamous Anonymous Whistleblower, Really Been Caught?*, WASHINGTON POST WORLDVIEWS BLOG (June 25, 2014), http://www.washingtonpost.com/blogs/worldviews/wp/2014/06/25/has-baba-jukwa-zimbabwes-infamous-anonymous-whistleblower-really-been-caught/

35 Babalo Ndenze *Call for Zuma Insult Law,* IOL NEWS (Nov. 15, 2012), http://www.iol.co.za/news/politics/call-for-zuma-insult-law-1.1423784.

SOUTH AFRICA

CENSORSHIP ON DEMAND

Failure of Due Process in ISP Liability and Takedown Procedures

Andrew Rens

A NEW STYLE OF CENSORSHIP

In South Africa, Internet service providers (ISPs) that host information are granted immunity against claims for hosting information, but only on condition that the service provider remove information on receipt of a complaint. Unlike other takedown regimes, such as that in the Digital Millennium Copyright Act, it is not confined to copyright; exemption from liability extends to any grounds of civil legal liability, while the potential subject of complaint is not restricted in any way.

Chapter XI of the Electronic Communications and Transactions Act, 2002 provides a 'notice-and-takedown' regime for South African hosting providers. Section 77, which provides for the content of the takedown notice and for liability for wrongful takedown, infringes freedom of expression and the right of access to court because it gives no opportunity for the poster of the allegedly infringing material to be heard on the matter by the ISP or a court before the material is taken down. The right of access to court is a type of due process right, enshrined in the Bill of Rights. The statutory regime fails the natural law requirements to 'hear the other side' and that 'no one may be judge in his own cause'. These natural law requirements are important in a determination of the constitutionality of the provision. Changes to the provision have been proposed as part of a larger overhaul of the statute in which it is included. Draft amendments to

the notice-and-takedown regime[1] similarly infringe freedom of expression and due process. As will be discussed either complete immunity for hosting service providers or a notice-and-notice regime would be more appropriate for the South African constitutional dispensation.

This chapter considers the statutory notice-and-take-down regime in South Africa as an example of the new version of censorship, in which private parties can effectively curtail freedom of expression by making use of the law, in this case a statutory self-help system that enables censorship through indirect means, through the interdiction of the means of communication.

SERVICE PROVIDER LIABILITY PROVISIONS AND THE TAKE-DOWN PROCEDURE IN SOUTH AFRICA

The hosting service provider liability and notice-and-takedown regime is set out in the Electronic Communications and Transactions Act 2002 (ECT Act) omnibus legislation passed in the early 2000s to deal with a wide range of online legal issues ranging from digital signature to encryption and computer crime. Chapter XI of the ECT Act, entitled 'Limitation of Liability of Service Providers' creates a regime that grants service providers exemption from legal liability provided that the service provider complies with the requirements of the chapter. Chapter XI covers a range of activities by service providers including hosting. Sections *75–77* in Chapter XI are intended to limit liability for service providers, including hosting providers because they provide a service that enables people to communicate efficiently with each other which results in a wide range of social and economic benefits, especially important to developing countries such as South Africa. Lowering the cost and other barriers to communication is thus important.

Internet service providers, including hosting providers are common carriers, just like telecommunications providers, railways and the like. South African law has never imposed liability on common carriers unless the corporation was actually party to a civil wrong or criminal offence. Imposing liability on ISPs, including hosting providers, would dramatically increase the cost of Internet access. Thus limiting service provider liability serves important policy goals. Globally, limitation of ISP liability is often accompanied by placing some requirements on service providers. The more onerous the requirements placed on service providers, the greater

the costs for ISPs, and those costs then form part of the cost of using the Internet for the customers of ISPs. Imposing onerous obligations on ISPs therefore raises the cost of accessing the Internet for ordinary South Africans, making it harder for South Africans to use the Internet to run businesses, access information, use government e-services and communicate with each other. How well do the legislative provisions governing hosting of information enable communication in South Africa?

Chapter XI of the ECT Act offers anyone providing information system services in South Africa a statutory shield against liability for communicating information. To qualify for exemption service providers must belong to a registered association with an approved code of conduct. Service providers that act as mere conduits and that provide caching services are simply exempt from liability.

Section 75 of the ECT Act mandates a more complex scheme for service providers which host data:

> *75. Hosting. —*
> *(1) A service provider that provides a service that consists of the storage of data provided by a recipient of the service, is not liable for damages arising from data stored at the request of the recipient of the service, as long as the service provider —*
>
> *a. does not have actual knowledge that the data message or an activity relating to the data message is infringing the rights of a third party; or*
>
> *b. is not aware of facts or circumstances from which the infringing activity or the infringing nature of the data message is apparent; and*
>
> *c. upon receipt of a take-down notification referred to in section 77, acts expeditiously to remove or to disable access to the data.*
>
> *(2) The limitations on liability established by this section do not apply to a service provider unless it has designated an agent to receive notifications of infringement and has provided through its services, including on its web sites in locations accessible to the public, the name, address, phone number and e-mail address of the agent.*
> *(3) Notwithstanding this section, a competent court may order a service provider to terminate or prevent unlawful activity in terms of any other law.*

(4) Subsection (1) does not apply when the recipient of the service is acting under the authority or the control of the service provider.

The exemption from liability in section 75 depends on compliance with section 77 of the ECT Act which provides:

77. Take-down notification. —
(1) For the purposes of this Chapter, a notification of unlawful activity must be in writing, must be addressed by the complainant to the service provider or its designated agent and must include —
a. the full names and address of the complainant;
b. the written or electronic signature of the complainant;
c. identification of the right that has allegedly been infringed;
d. identification of the material or activity that is claimed to be the subject of unlawful activity;
e. the remedial action required to be taken by the service provider in respect of the complaint;
f. telephonic and electronic contact details, if any, of the complainant;
g. a statement that the complainant is acting in good faith;
h. a statement by the complainant that the information in the take-down notification is to his or her knowledge true and correct; and
(2) Any person who lodges a notification of unlawful activity with a service provider knowing that it materially misrepresents the facts is liable for damages for wrongful take-down.
(3) A service provider is not liable for wrongful take-down in response to a notification.

If a service provider fails to comply with the requirements of sections 75 and 77 that failure does not establish any liability but merely removes one possible defence that a service provider could raise to a claim. As a consequence, a hosting service provider does not need to prove that its liability is limited by the ECT Act if there is no liability in South African law. However, it does give hosting service providers which remove information an absolute defence against claims by those who have used the service provider's services to host information.

A hosting provider is not legally obliged to remove the material that is the subject of a complaint. Refusal to remove information will only result

in loss of the statutory grant of exemption from liability. Exemption from liability is not necessary when there is no liability in the first place. A service provider can only be held liable if two conditions are met. First the posting of the information by the person posting it must give rise to liability for that person; for example, the user could infringe a right to privacy, defame someone or infringe copyright. Second, if the person using the service is liable on some legal grounds, there must also be a legal rule extending the user's liability to the service's provider.

The issue of whether hosting information gives rise to liability hasn't been decided by a court in any of the categories in which such claims might be made — such as trademark, trade secret, copyright, defamation, privacy, or the like. The provisions of the ECT Act themselves do not explicitly require that the complaint contain a legal basis for liability. If a hosting provider fails to comply with a complaint, even if it is baseless, it loses the exemption from liability provided in the ECT Act. However, investigating whether there is an underlying basis for liability and taking the risk of possible liability imposes costs on the provider. It is far cheaper and less risky for a hosting provider to routinely take down any material it has been requested to remove.

Thus hosting service providers have a legally-structured incentive to prevent speech that would otherwise take place by removing information on any complaint. Service providers, whether modelled as rational wealth maximisers or predictably irrational risk avoiders, have strong incentives — and no disincentives — to remove information on receipt of a complaint without any investigation into the merits of the complaint or assessment of the legal basis of the complaint. A person who made use of the service to communicate information is entirely cut out from the process, as are all persons who would receive the information, or would wish to do so.

CENSORSHIP BY TAKEDOWN

Can the interdiction of the means of speech be characterized as censorship, when it is carried out by one non-state actor at the behest of another? While all types of service providers enjoy statutory exemption there is no explicit statutory must-carry rule. However, the architecture of the Internet requires service providers to communicate all traffic indiscriminately.

Depending on the service provided, the architecture of the Internet may require a service provider to not only transmit communications to and from its customer but also pass on information that is en route elsewhere.[2] The result is a means of communication vastly more efficient and pervasive than any preceding system.

One important part of this system is the World Wide Web (henceforth, 'the Web'). In order to receive communication via the Web a person needs a suitable device connected to the Internet. To speak via the Web, a person must either run her own server, which is well beyond the technical capacity and technological resources of most people, or speak only on websites provided by others, such as social network services, or contract with a hosting provider to host her website. Speaking via the Web is thus possible only with the cooperation of a hosting provider or with the cooperation of someone else who in turn relies on a hosting provider. A hosting provider thus has a great deal of power over the ability of its customers to communicate, but it does so only because multiple others; service providers, telecommunications network operators, software engineers all cooperate through adhering to the engineering standards of the Internet.

The layers of the communications networks making up the Internet are together very much more valuable than any single part, both economically and socially. Hosting providers thus profit from a type of commons,[3] but also control access to that commons. This might have been sufficient reason for South African courts to extend a common law remedy that prohibits disconnection of water, electrical supplies and even connection to a telecommunications network without a court order to service providers, including hosting providers.[4] Instead, the legislature has intervened by both creating, whether intentionally or otherwise, incentives for services providers to remove content — effectively silencing speech — as well as exemption from liability for doing so.[5] Far from tempering the power of hosting providers, the State has increased it and has biased it towards silencing speech.

As it stands, section *77* enables censorship of speech by both government and private actors. This may be illustrated by way of a hypothetical. If a union created a website in support of a strike and parodying the name or slogan of the employer, then could the employer claim that the parody is damaging to its reputation or infringing of its trademarks?[6] Under the

ECT Act, the employer could send a notice to the service provider hosting the website alleging that its rights are infringed. Under the current system the hosting provider would have every incentive to remove the website in order to avoid liability. The complainant might even have a good faith belief in the validity of his complaint but he is disqualified from making an impartial assessment of his complaint. The provisions do not require that the union official be given notice, nor be given an opportunity to make representations before her right to freedom of expression is stifled. The way in which the statutory scheme empowers complainants at the expense of service providers has raised policy concerns, leading to amendments proposed to the statute.

PROPOSED AMENDMENT TO INTERMEDIARY LIABILITY

In 2012, the government department charged with administration of the old ECT Act reviewed multiple aspects of the Act. The cabinet minister responsible for the department stipulated that "any notice or take-down procedure should allow for the right of reply in accordance with the principle of administrative justice and the *audi alteram partem* rule."[7] Why should the principles of administrative justice, otherwise known as natural justice, apply? The executive seemingly acknowledges that the takedown provisions are state intervention into relations between non-state actors. Natural justice is required in highly-regulated relationships such as employment relationships; given that the relationship between a subscriber and an Internet service provider is regulated by Chapter XI of the Act in a way that substantially affects the power of the parties *inter se*, it ought to be seen as a highly-regulated relationship, and the principles of natural justice ought to be observed.

In response to the minister's concerns, the department drafted proposed amendments to the scheme. Briefly: a complainant sends a notice to a hosting service provider, which in turn must reply on the substance of the complaint within ten days, after which the complainant decides whether to insist on takedown, which she communicates through a further notice. The proposal burdens the hosting service provider with making a case for the original poster of the content. There is still no provision that posters be afforded an opportunity to be heard, or even be informed, of the process. The departmental response to the minister misconstrues who should be afforded an opportunity to be heard. It is the poster's

speech that is curtailed, and not the hosting provider's speech; therefore the poster should be allowed to be heard. Both the current legislation and the proposed amendments thus contravene the requirements of natural justice.

"The core requirements of natural justice are the need to hear both sides (*audi alteram partem*) and the impartiality of the decision maker (*nemo iudex in causa sua*)."[8] Both the current legislation and the proposal empower the complainant to decide whether or not his complaint justifies curtailing the speech of another person. Under the current legislation the service provider must decide whether to take down information; pitting its own interests in avoiding liability to the complainant and reducing its costs of responding to disputes, against the rights of the person who posted the information, often a subscriber to its services. The service provider has no duty under the statutory scheme to act impartially while taking the decision to take down the information, although it can be argued that the service provider has relevant constitutional duties.

At the same time the service provider enjoys statutory immunity against claims by the poster of the information for taking the information down. As a result, service providers are likely to act in their own interests and take down information. A study of service provider responses to takedown notices in India, where a similar law exists, shows that the majority of service providers take down information regardless of legal validity of the underlying complaint.[9] The service provider is under no obligation to give a reasoned decision for its decision to remove the information. While it is possible to create a statutory scheme in which a service provider might decide whether or not to take down information in a way that meets the requirements of natural justice the current legislation fails to meet the requirements of natural justice.

The proposed legislation permits a complainant to send a complaint to the service provider requiring takedown, the service provider is required to respond. Thereupon, according to the proposed section 77A:

> *(3) The complainant shall give due consideration to the response from the service provider and may if the complaint has not been resolved to the satisfaction of the complainant issue a final take-down notice to the service provider within a further 10 business days.*

(4) A service provider who does not comply with a final take-down notice within a further 10 business days may be liable for a related offence.

Under the proposed amendment, the complainant effectively decides whether his interests should override the rights of others, including freedom of expression, the right to receive information, and the right of the subscriber to receive services for which she has paid. The proposed amendments vest the final decision to take down the information in a party with an expressly-stated interest in taking the information down. Thus, it violates the natural law requirement that decisions that involve disputes of right should not be decided by a party with an interest in the decision, a requirement that animates the natural law principal *nemo iudex in sua causa;* that no one may be judge in his own cause.

The failure to enable the poster of the information to be heard violates the *audi alteram* rule. Even if a complainant were able to make an objective decision others affected by the decision would regard the complainant as biased by her own interests, and there would thus be perception of injustice contrary to the principle that justice must not only be done but be seen to be done.[10] The failure to comply with principles of natural justice does not by itself enable a common law challenge to the legislation, however it is relevant both to the legislative amendment process and to the constitutionality of the censorship scheme.

CONSTITUTIONAL ANALYSIS

Any law passed in South Africa must accord with the Bill of Rights, if it does not then it is invalid,[11] and is liable to be declared invalid by a court at some point. It is therefore important to consider the constitutional requirements that affect the imposition of requirements on service providers. Two important rights that must be taken into account are the rights of freedom of expression and access to court. The right to freedom of expression is set out in section 16 of the Bill of Rights in the Constitution.

16. Freedom of expression. —
(1) Everyone has the right to freedom of expression, which includes —
(a) freedom of the press and other media;
(b) freedom to receive or impart information or ideas;
(c) freedom of artistic creativity; and

(f) academic freedom and freedom of scientific research.

(2) The right in subsection (1) does not extend to —

(a) propaganda for war;

(b) incitement of imminent violence; or

(c) advocacy of hatred that is based on race, ethnicity, gender or religion, and that constitutes incitement to cause harm.

Freedom of expression includes not only the right to impart information but also to receive it. Any limitation on means of communication exchange thus implicates rights of those seeking to receive information as well as those intent on imparting it.

The Constitution requires that laws such as the ECT Act must restrict the right to freedom of expression as little as possible. Service providers are obliged to uphold the right to freedom of expression of those persons whose information they host, an obligation that precedences and overrides any statutory obligation. Section 8 of the Bill of Rights states:

8. Application. —

(1) The Bill of Rights applies to all law, and binds the legislature, the executive, the judiciary and all organs of state.

(2) A provision of the Bill of Rights binds a natural or a juristic person if, and to the extent that, it is applicable, taking into account the nature of the right and the nature of any duty imposed by the right.

The only practical way for many South Africans to exercise their freedom of expression beyond their immediate environs, as also to receive information and access a wider body of knowledge, is by means of the Internet. Internet access is therefore a core freedom of expression issue. Therefore, any procedure established by the ECT Act that prevents speech — such as the notice-and-takedown scheme of section *77* — should take into account the obligation placed on service providers to respect the freedom of expression of others. The right of access to court, as guaranteed by Section 34 of the Bill of Rights, must also be taken into account.

34. Access to courts. —

Everyone has the right to have any dispute that can be resolved by the application of law decided in a fair public hearing before a court or, where appropriate, another independent and impartial tribunal or forum.

The consequence of section 34 is that any procedure to address disputes in the ECT Act must enable a court or other impartial body to make the decision that affects the rights of any person. This is especially important when a dispute may affect the rights in the Bill of Rights such as the right to freedom of expression. However, section 77 places the decision to remove the information in the hands of the complainant. This is a form of 'self help' that is not permitted in the South African constitutional dispensation. In *Lesapo v. North West Agricultural Bank*[12] the Constitutional Court held that:

> *Section 34 and the access to courts it guarantees for the adjudication of disputes are a manifestation of a deeper principle; one that underlies our democratic order. The effect of this underlying principle on the provisions of section 34 is that any constraint upon a person or property shall be exercised by another only after recourse to a court recognised in terms of the law of the land . . . . In a modern constitutional state like ours, there is no room for legislation which, as in this case, is inimical to a fundamental principle such as that against self help. This is particularly so when the tendency for aggrieved persons to take the law into their own hands is a constant threat.*
>
> *This rule against self-help is necessary for the protection of the individual against arbitrary and subjective decisions and conduct of an adversary. It is a guarantee against partiality and the consequent injustice that may arise.*[13]

A complainant therefore cannot be allowed to decide on the exercise of rights of freedom of expression by other persons. A service provider is also not appropriately equipped to decide disputes about freedom of expression, and itself has interests in any dispute, not least of which are reducing costs of disputes and avoiding liability. Section 77 as it currently stands, as well as the proposed changes to section 77, limit freedom of expression by authorizing anyone to issue takedown notices to service providers that prevent expression by speakers and prevent receipt of information by those who want to receive information and ideas.

The South African notice-and-takedown regime infringes the right of access to court. A complainant is able to effectively require the service provider to remove information without a court order. It is important to

be clear about which dispute is prevented from being heard by a court. The dispute that the court is precluded from hearing is not a dispute between the complainant and the speaker about whether the information infringes a right of the complainant but instead the dispute about whether the service provider should remove the information.

The provisions do not in themselves prevent a speaker from approaching a court to order that the ISP should again make available information that it has taken down. A speaker providing information could theoretically approach a court because her rights have been infringed.

However, since the provisions do not require that the service provider give the speaker any notice of the takedown, how would the speaker know why the information has been removed? But even if a speaker were able to find out that the removal was at the behest of the complainant what could she hope to obtain from a court? A speaker could not claim damages against a service provider even for a takedown due an absurd claim because section *77*(3) of the ECT Act bars such a claim. Would a court be willing to order a service provider to host information? Even if court did make such an order, it could be rendered ineffective because the complainant could once again issue takedown notices, and once again the service provider would have to comply or face potential liability.

Section *77*(2) creates liability for a person who materially misrepresents facts in a complaint as a potential remedy for a person who has sought to use the Internet to communicate but had that communication silenced by a complaint. Significantly the statute does not impose liability on a complainant who makes an invalid legal claim based on valid facts but incorrect legal reasoning. In the example already discussed, if the employer objects to the use of its trademarked slogan by the trade union, it might complain that the trade union is reproducing a copy of its trademark. That the trademark was being reproduced would be a correct fact however the claim by the employer that the trade union is barred from reproducing the trademark is a misinterpretation of trademark law. If the employer were wrong in its claim about the legal consequences of the fact, the union official would not be able to claim damages according to the provisions, since it only provides damages if there is a misrepresentation of facts. Moreover, in the event that there is a valid complaint, the statute removes the claim

altogether so that any legal claim could be regarded as more important than freedom of expression and access to court.

A complaint based on trademark would thus mandate removal of a parodic use of a trademark even if there were important freedom of expression concerns at stake.[14] The basis for the damages which a silenced speaker might claim is at best equivocal. Does the sub-section create a new category of statutory damages? If so, what is basis for calculating those damages? Or must a silenced speaker prove that she suffered damages as the result of a common law delict?[15] Or is it intended that she might claim constitutional damages for infringement of her information rights? Must the misrepresentation be intentional, or would a negligent misrepresentation give rise to damages? None of these questions has a clear answer.

Together sections *75* and *77* create an automatic injunction against speech on the Internet hosted by South African ISPs. The sections place the burden of approaching a court on the party seeking to exercise her constitutional rights of expression rather than on the person seeking to limit another's information rights. Read together, sections *75* and *77* limit the right of freedom of expression, the right to receive information and the right of access to court. While it is constitutionally permissible possible to limit the rights provided in the Bill of Rights, any law that does so must comply with section 36 of the Bill of Rights, which, *inter alia*, requires that there be no "less restrictive means to achieve the purpose".[16]

If a person is to be barred from using the Internet to exercise her information rights is there an alternative means by which she might do so? Although the takedown regime does not absolutely bar a person from expressing herself there is no alternative means to the Web (at least for the vast majority of South Africans) that will enable a person to communicate as efficiently, especially over time and distance.

An important factor in a section 36 constitutional analysis of sections *75* and *77* of the ECT Act is whether there are processes that achieve the purpose but which is less restrictive means to achieve the same ends. There certainly are less restrictive means of achieving the purpose of providing immunity to service providers. One obvious means would be to extend the unconditional immunity conferred on other types of service providers by the ECT Act on content hosting providers. Anyone with a

legal claim against a speaker can approach the institution best suited to testing the validity of the claim: the courts. Other less restrictive means include notice-and-notice provisions, and similar provisions in use in other countries.

In 2012, Canada passed a dealing with the liability of providers of 'communications networks' for copyright infringement.[17] Canadian law is of particular importance because the South African Bill of Rights is modelled on and in many aspects resembles the Canadian Charter of Rights and Freedoms. The Canadian provisions,[18] encode long-standing practice in Canada. A service provider which receives a notice from a complainant must give notice to an alleged copyright infringer, and keep certain records in respect of the infringement for a set period to facilitate litigation. The complainant must pay a fee to the service provider for these actions. The liability of the service provider is confined to a statutory damages claim with a limit set by regulation. Providers of information location tools are exempt from any order other than an injunction.[19]

A court may give an order to a service provider to remove information, however in doing so it must take into account a number of factors including the aggregate effect of the injunction with any injunctions from other proceedings, the technical feasibility of implementing the order, the burden on the service provider and the availability of less burdensome and comparably effective means of preventing or restraining the infringement. The South African legislature could adopt a simplified notice-and-notice regime in which the complainant would give notice to the hosting service provider, who in turn would notify the poster of the information. The poster would then decide whether or not to oppose the complaint, if so the hosting service provider would notify the complainant who could then approach a court for an interdict (injunction).[20]

CONCLUSION

The deficiencies of the current South African notice-and-takedown regime for hosting service providers led to a proposal, in December 2012, by the government department responsible for the statute to amend the provisions. The proposed change would require hosting service providers to respond to complainants who could still insist that the material or content be taken down. There is no express provision for the service provider to

notify the poster of the content of the takedown notice or to afford him a chance to respond to the takedown notice. It is left up to service providers to determine for themselves how to best proceed. The proposed amendment is thus no better than the current provisions. Since the proposed amendments do not safeguard freedom of expression and the right to due process of those who furnish information they probably would not save the regime from being declared unconstitutional.[21]

The current notice-and-takedown regime has not resulted in a single court case. This is not surprising since speakers are ignored in the statutory process, and are instead confronted with a *fait accompli*. One result of this is that the courts have not had an opportunity to rule on whether ISPs are liable for the protected speech of their customers, and if so under what circumstances. While an ISP can choose to take down information or take a risk of liability, it has strong incentives to remove information. The statute thus creates incentive for a type of conduct that in practice limits freedom of expression. Section 2 of the South African Constitution prohibits unconstitutional conduct as well as laws. A law that encourages, even if it does not require, unconstitutional conduct can therefore readily be found to be unconstitutional.

Sifting through the factual representation by complainants, assessing the validity of their legal claims, and balancing those against the fundamental rights of speakers and their audiences are complex tasks. Neither complainants themselves nor ISPs are equipped for them.

Courts, on the other hand, are constituted precisely for these kinds of tasks. The obvious solution is that disputes about information online must go to court, and the way to ensure that they go to court is to grant ISPs greater immunity for keeping information available so complainants pursue their claims against speakers in courts.

1 See proposed amendments to section *77* in the proposed Electronic Communications and Transactions Amendment Bill (26 October 2012).

2 *See generally* Lawrence Lessig, The Future of Ideas (2001) (Part I of that book has a detailed discussion on the way in which the Internet operates and its implications for legal regulation).

3 *Id.*

4 *See generally* Andrew Rens, *Telkom SA Limited v Xsinet (Ptoprietary) Limited,* 120 SALJ *749* (2003).

5 Section *77*(3), Electronic Communications and Transactions Act.

6 This example is suggested by an incident reported in the press. The South African subsidiary of Barclays Bank was engaged in a dispute with the trade union Solidarity which represented bank staff. Solidarity created a website www.stopabsa.co.za that included a logo with the words 'Today, Tomorrow, Goodbye'. The logo was a parody of the bank's logo 'Today, Tomorrow, Together'. The bank threatened legal action to have the site closed down because of the parody. S*ee*, I-Net-Bridge, *Legal Threat Against Stop ABSA Website,* MyBroadband (Mar. 29, 2012), http://mybroadband.co.za/news/banking/46794-legal-threat-against-stop-absa-website.html.

7 Memorandum on the Objects of the Electronic Communications and Transactions Amendment Act ¶ 12.5, GN 888 in GG 35821 of 26 Oct. 2012 (S. Afr.).

8 County Fair Foods (Pty) Ltd v. Theron N.O. & Others 2000 (21) ILJ 2649 (LC) at 2652–3, *aff'd in* Raswiswi v. Commission for Conciliation Mediation and Arbitration & Others 2011 (32) ILJ 2186 (LC), and drawing on Lawrence Baxter, Administrative Law 536 (1984).

9 Rishabh Dara, Intermediary Liability in India: Chilling Effects on Free Expression on the Internet (2011), http://cis-india.org/internet-governance/intermediary-liability-in-india.pdf

10 *See* R. v. Sussex Justices, *ex parte* McCarthy, [1924] 1 KB 256; this principle has been accepted by South African courts.

11 Section 2, S. Afr. Const., 1996, states: "This Constitution is the supreme law of the Republic; law or conduct inconsistent with it is invalid, and the obligations imposed by it must be fulfilled."

12 2000 (1) SA 409, ¶ 16.

13 *Id.* ¶16–18.

14 This result would be in direct conflict with the decision of the Constitutional Court in the seminal case of *Laugh It Off Promotions CC v. South African Breweries International (Finance) BV t/a Sabmark International & Another*, 2006 (1) SA 144 (CC), in which the court upheld the right to create and sell apparel that parodied trademarks to make political arguments. In a landmark series of cases that started in the Western Cape High Court and were appealed to the Supreme Court of Appeal, and finally to the Constitutional Court, South African Breweries persisted in its claim that t-shirts distributed by Laugh It Off were tarnishing their trademark for beer. The Constitutional Court ruled otherwise. Most South Africans do not have the means to approach the Constitutional Court to vindicate their right to freedom of expression, as Laugh It Off did.

15 Delict is the South African common law term equivalent to tort in the United States or United Kingdom.

16 Section 36(1)(e), S. Afr. Const., 1996. The full section reads:

> *36. Limitation of rights. —*
> *(1) The rights in the Bill of Rights may be limited only in terms of law of general application to*

the extent that the limitation is reasonable and justifiable in an open and democratic society based on human dignity, equality and freedom, taking into account all relevant factors, including —

(a) the nature of the right;

(b) the importance of the purpose of the limitation;

(c) the nature and extent of the limitation;

(d) the relation between the limitation and its purpose; and

(e) less restrictive means to achieve the purpose.

(2) Except as provided in subsection (1) or in any other provision of the Constitution, no law may limit any right entrenched in the Bill of Rights.

17 Copyright Modernization Act, Bill C-11 (Can.).

18 Copyright Act, R.S.C. 1985, c. C-42, s.41.25-26 (Can.). The provisions in respect of communications network service providers were not yet in force as of August 2014.

19 *Id.* 41.27.

20 The author of this chapter wrote a response to the draft bill setting out how a simplified notice-and-notice regime might operate, which was endorsed by the Association of Progressive Communications. See Andrew Rens, Section 77: Service Provider Liability and Take Down Procedures (Representation on Amendment by Andrew Rens) 13–17, http://www.apc.org/en/system/files/Submission_on_section_77_byAndrewRens.pdf.

21 *Id.* at 12.

SRI LANKA

CENSORSHIP THROUGH FORENSICS

Video Evidence in Post-War Crises

Rebecca Wexler[1]

INTRODUCTION

In the digital era, communications intermediaries sometimes play the role of censor. This Chapter considers how censorship through communications intermediaries operates in the domain of forensic video analysis (FVA). Anonymous video shot on mobile devices worldwide and posted online is helping to hold authorities to account for police misconduct, war crimes, and other abuses of power.[2] What happens when the authenticity of that video is in doubt? The possibility of justice depends on forensic investigators who sometimes shroud their tools and methods in secrecy, disabling scrutiny of their authenticity claims.

This chapter argues that secrecy as well as other forms of proprietary restrictions on access to FVA tools and methods constitute a form of censorship because they create obstacles to the reproducibility of experimental results, undermining scientific authority. These obstacles generate both procedural and material restraints on speech. Procedural censorship interferes with the means of speech production. Material censorship proscribes the substance of expression. To illustrate the production of material and procedural censorship through forensics practices, the Chapter examines a dispute over the authenticity of a leaked video depicting alleged war crimes in Sri Lanka.

During the critical moments of post-war transition in Sri Lanka, after

thirty years of ethnic conflict and civil war, a television network in the United Kingdom (UK) broadcast an anonymous video depicting men in Sri Lankan military uniforms shooting naked, bound prisoners in the head. The video provoked pained public outcries and became a focal point for frustration, mistrust, and controversy surrounding post-war self-making and national re-formation. Lack of clear public consensus regarding its authenticity aggravated the controversy. Some believed that a soldier in the Sri Lankan military recorded the video on a cell phone while witnessing—and perhaps perpetrating—an extrajudicial execution.[3] Others suggested that the video might depict a fictional scene with actors and fake blood, produced by a commercial film crew intent on discrediting the Government of Sri Lanka (GoSL).[4]

Forensic analysts failed to resolve the confusion. Experts working at the request of the United Nations (U.N.) found evidence of authenticity strong enough to warrant investigation into possible war crimes.[5] Yet experts working on request of the GoSL found evidence that the video is either inauthentic or unverifiable.[6] As a result,[7] the GoSL declined to investigate the incidents depicted.[8]

I collaborated with a forensic scientist and court-appointed Special Master for multimedia evidence, Dr. Rich Murphey, to produce the first independent audit of the forensic reports on both sides of this controversy.[9] We found intermediary obstacles to the reproducibility of the experiments that both U.N. and GoSL researchers relied upon to evaluate the video's authenticity. These obstacles arose from incomplete documentation, proprietary conflicts of interest, and explicit secrecy. This chapter presents our results.

Our audit shows how obstacles to reproducibility in experiments can operate like prior restraints on scientific counter-speech. Traditional prior restraints require government approval for speech before it happens.[10] Similarly, restricted access to forensic tools and methods means that potential speakers need ex ante permission to practice the instruments and techniques of speech — procedural censorship.

Obstacles to reproducibility also constrain the substance of expressions — material censorship — because they inhibit broader publics from reaching consensus around experimental conclusions. In FVA disputes,

these obstacles can annul the public meaning of video evidence. The effect is to censor meaning, rather than to block the flow of information, and hence to obstruct access to knowledge in the most profound manner. In other words, censorship here manifests by rendering incomprehensible that which is in plain sight.

As digital information products become increasingly uncontainable, effective censorship may nonetheless be possible by blocking access to the tools and methods of analysis that produce meaning from widely available information. The censorial result is to render meaningless the information that has become uncontainable. Moreover, as the Sri Lanka video dispute illustrates well, the culturally-sanctioned halo of objectivity that surrounds science and technology makes that sphere a likely site for this type of willful manipulation of consensus-based public truths.

Resistance against this form of censorship will depend on publics' ability to scrutinize expert claims. As a result, this chapter advocates that the emergent field of FVA adopt open tools and methods, incorporating the opportunity for investigators to observe and analyse all levels of functionality.

Part I considers the role of reproducibility in producing scientific authority, as well as the urgency of reproducibility for authenticity investigations into anonymous online video speech in particular. It draws on understandings of the construction of scientific authority developed by historians and philosophers of science and connects these concepts to ongoing debates in legal academia about the role of material objects and intermediaries in digital era censorship. The ongoing controversy over the authenticity of the Channel 4 video, described in Part II, makes visible contestation over objectivity production within FVA and the struggle to achieve scientific consensus in a cross-cultural environment. FVA here serves divergent visions of community boundaries and national and international priorities. A detailed technical audit of the FVA reports, presented in Part III and deeply indebted to Dr. Murphey's expert contributions, documents obstacles to the reproducibility of the forensic investigations into the Channel 4 video. Part IV concludes with a plea for the development and adoption of open tools and methods in the emergent field of FVA in order to stem the force of censorship through forensics.

CENSORSHIP, SCIENTIFIC AUTHORITY, AND EXPERIMENTAL REPRODUCIBILITY IN FVA INVESTIGATIONS

Censorship Through Communications Intermediaries

Censorship increasingly operates indirectly via influence over the means of digital communication rather than through direct penalties or injunctions against expression.[11] Moreover, unruly digital information and accompanying cultures of transparency have increased authorities' reliance on material constraints, such as Internet filters, to perform the role of the censor intermediary.[12] In fact, as law professor Jack Balkin expressed particularly well during a recent symposium on the U.S. First Amendment, early twentieth-century states enforce "new-school" censorship through the same online intermediaries that simultaneously provide the "infrastructure of free expression."[13]

Communications intermediaries can also generate independent *de facto* censorship, absent or even contrary to state pressure. Law professor Marvin Ammori shows, for instance, that lawyers for global Internet businesses agglomerate corporate goals, international laws, and foreign traditions into their terms of use, and thereby in effect "write the rules governing our speech."[14] For similar reasons, law professor Mark Tushnet suggests that independent censorship by speech intermediaries should perhaps be subject to regulation under the state action doctrine, which extends constitutional governance to private parties performing in the role of the state.[15] These issues are prevalent across jurisdictions.[16]

Censorship Through Obstacles to the Reproducibility of Scientific Experiments

I suggest that like Internet filters or communications service providers, the tools and methods of scientific experiments are information intermediaries. These tools and methods are the essential means to generate and disseminate scientific speech. As a result, they are also likely sites for censorship. Restrictions on access to experimental tools and methods function as a form of censorship by interfering with the means of producing scientific authority.

The construction of scientific authority depends on the reproducibility, or at the least the plausibility of replicating, scientific experiments. Experimental findings gain credibility when a different investigator, similarly

equipped and following the same procedures, produces the same results.[17] As historians and philosophers of science have shown, this ideal that scientific experiments should be replicable in principle underlies the consensus-based construction of facts.[18] Restrictions on access to experimental tools and methods produce obstacles to reproducibility. These obstacles interfere with the creation, expression, and adoption of scientific speech. In sum, restricting access to scientific tools and methods can produce a form of censorship.

Censorship Through Forensic Video Analysis

Applying the concept of censorship through communications intermediaries to Forensic Video Analysis (FVA) shows the urgency of reproducibility for investigations into the authenticity of anonymous online videos.

Current FVA methods are inadequate, with strategies drawing primarily on forensic techniques developed for digital stills. These still image digital forensics techniques may look for, for example, irreversible footprints of digital processing steps within an image. Analysts can then attempt to reverse engineer these steps to reconstruct the circumstances of first-generation production of that image. Researchers may hope through this method to determine the mechanical source of a still image, including the camera model and vendor, whether an image has been manipulated via cut-and-paste operations, and the processing history of an image.[19]

But leading researchers in the field caution that "the peculiarities of video signals" thwart easy application of still image forensic techniques to FVA.[20] Digital manipulation of a video can apply both to single frames, which appear twenty-four to thirty times per second, and to the temporal alignment of frames within a sequence. In short, video data is of a different order of magnitude from stills. Further, the high compression ratio of most video formats can erase footprints left by signal modification, making it difficult or impossible to reconstruct a video's processing history.[21] FVA is, unmistakably, an emergent discipline with unresolved issues.[22]

At the same time, that digital video itself is infinitely reproducible without risk of degradation throws an unprecedented burden on the authority claims of forensic analysis. In comparison, physical evidence such as blood or fingerprints is limited by its own material nature. Physical

samples that are collected from a crime site and tested by one investigator cannot be recollected and tested by another. These limits mean that the number of forensic investigators who may access the samples and proffer expert opinions about them remains small.

The same does not extend to video.[23] The Channel 4 videos, for example, are broadly accessible and easy view or download from the Internet. Decision-makers throughout publics and governments can access their own copies. As a result, they may be more likely to incorporate their own analyses into their determination of authenticity rather than accept the conclusions of a forensic report on expert authority alone.

What is more, several competing paradigms exist beyond FVA for the authentication of video evidence. News organizations may triangulate verification from multiple sources prior to publication.[24] Genre expectations can influence an individual's trust in the veracity of an image.[25] And personal experience with the tools of video production, such as cell phone cameras and home editing software, contributes a broad base of technological literacy against which decision-makers may measure authenticity claims.

As a result, at this moment in the specific and newly developing field of FVA, interests in the reproducibility of experiments should outweigh proprietary interests in restricting access to tools and methods. To be sure, public science policy must balance principles of reproducibility against competing interests. On one hand, peer and market competition, on which much scientific knowledge production depends, can mandate a minimal level of secrecy around investigative methods and procedures.[26] On the other hand, as historian Sheila Jasanoff has written, democracy mandates that the polity have some means with which to evaluate "knowledge claims that justify actions taken on its behalf."[27]

Reproducibility of investigative procedures is crucial to generate consensus in the current video evidence environment of decentralized access and knowledge, competing authentication paradigms, and existing limitations within the FVA discipline. Rigorous commitment to the production of transparent investigative procedures, and technologies open to scrutiny, will both strengthen current FVA standards and also facilitate public trust in the future credible authority of FVA investigations.

THE VIDEO DISPUTE

On Tuesday, May 19, 2009, Sri Lanka celebrated the end of thirty years of civil war. Lieutenant General Sarath Fonseka, commander of the Sri Lankan army, announced, "We have liberated the whole country from terrorism."[28] The government of Sri Lanka (GoSL) had defeated the Liberation Tigers of Tamil Eelam (LTTE), an insurgent group designated a terrorist organization by the United States and thirty-one other countries.[29] Sri Lanka's High Commissioner in London proclaimed the defeat the first victory against terrorism in the modern age.[30] Sri Lanka began to navigate a complex post-war scenario.

Yet, the celebratory narrative soon fractured. On August 25, 2009, Channel 4 News in the UK broadcast the leaked video that would become the subject of international dispute. Channel 4 acquired this video, approximately one minute long, from Journalists for Democracy in Sri Lanka (JDS), which in turn obtained it on condition of the total anonymity of its source.[31] On December 2, 2010, Channel 4 released a second, longer video of approximately five minutes in length, which appears to contain the contents of the first.

The unknown provenance of these video complicated efforts to authenticate them.[32] Authenticity here refers to the veracity of the scene depicted in an image, rather than the integrity of the image itself.[33] Without an unbroken chain of custody from an original and identifiable producer, speculation flourished about the circumstances of the videos' creation.

Forensic analysts sought to resolve these speculations by examining the video files for traces of image manipulation. Digitally altered portions of a frame, or a match between a video file and the type of light sensor only present in large commercial cameras, would discredit the video as a cell phone recording of an historical incident. Absence of such manipulation, or a match between a video file and the type of light sensor only present in cell phone cameras, would support the opposite assumption of authenticity. In analyses of both videos, U.N. investigators found evidence of authenticity, while GoSL found them inauthentic and, as noted above, declined to investigate the incidents depicted.[34]

Subsequent leaks of additional photographs and videos portraying similar scenes from other incidents did not alter the GoSL's stand.[35] Mean-

while, controversy surrounding the initial videos continues.[36] Accountability for possible war crimes, on the one hand, meets on the other hand a possible double standard as to which nations face such allegations in the first place. At stake is the GoSL's ability to obtain foreign aid, in addition to its legitimacy in the eyes of its own population. The opportunity to construct a stable peace hangs in the balance.

EVIDENCE OF CENSORSHIP THROUGH FORENSICS: OBSTACLES TO REPRODUCIBILITY IN THE CHANNEL 4 VIDEO FVA REPORT[37]

Obstacles to the reproducibility of experimental tools and methods appear in both the GoSL and U.N. investigative reports. Indeed, the dispute began with an obfuscation of investigatory methods. On September 9, 2009, GoSL forensic analysts sent the U.N. their conclusion that the video is a fake, but omitted documentation of the investigations behind this finding.[38] The U.N. then repeatedly requested the full texts of their investigative analyses, but GoSL investigators did not provide them until 2011, two years later.[39] Unfortunately, procedural obfuscations and barriers to reproducibility only grew from here.

Incomplete Documentation as an Obstruction to Experimental Reproducibility

Incomplete documentation regarding evidence preservation cast doubt on whether or not all of the investigators actually analysed identical copies of the videos. Researchers may employ a cryptographic hash to verify their copy of a digital file. The hash algorithmically generates a number to uniquely identify the content of a digital file.[40] Anyone who runs this algorithm and produces the same numeric identifier can determine that they have an unaltered copy of the file.[41] Yet, none of the U.N. and GoSL FVA reports includes a hash.[42]

At least one investigator attributed omission of the hash to the anonymity of the original videographer.[43] True, a hash under these circumstances would not have established preservation of the evidence from a first-generation source. Still, the unknown nature of the source does not excuse the omission. Rather, the opposite is true. Multiple second-generation sources for the videos under investigation mean a hash would have been particularly useful. A hash would have clarified whether or not all the FVA investigators were analysing the same video files, which is a pre-

requisite to reproducibility. Absent this foundational piece of information, none of the parties can challenge or accept the conclusions of the others. Scepticism as to whether all parties analysed the same piece of evidence renders any consensus about its authenticity meaningless.

In fact, there are strong reasons to doubt that all of the investigators did actually examine unaltered copies of the videos. In the first round of reports on the initial, — shorter — video, U.N. and GoSL investigators each described analysing videos of different lengths, names, and formats, while GoSL investigator Chathura De Silva reported difficulty obtaining a copy of the video at all.[44] De Silva described the video he eventually analysed as, "an available streaming media source on the Internet, which had been trans-coded several times and lacked most of the forensic features."[45] Had a cryptographic hash been used, investigators would have known if they were analysing fragments or the whole of the same piece of evidence or not, regardless of their source.

A second round of investigations ameliorated some of this confusion. This round followed the release of an extended version of the video, approximately five minutes in length, which appears to contain the contents of the first. Christof Heyns, the U.N. Special Rapporteur on Extrajudicial Executions, reports that he distributed this video to both U.N. investigator Jeff Spivack and to the GoSL.[46]

However, despite the promising start of a shared source, discrepancies abound. Spivack identifies the video file as "SL1.3GP", and sources it to Heyns.[47] U.N. investigator Grant Fredericks identifies it by the same name, but sources it to Mr. Orest Nowasad from the U.N. Office of the High Commissioner for Human Rights, rather than to Heyns, and adds that it is five minutes and twenty-five seconds in length.[48] Two pages later, Fredericks changes his length approximation to five minutes twenty-four seconds.[49] He also establishes that he will re-examine the initial, shorter video, which he first identified as one minute and seventeen seconds but now claims is one minute and fourteen and a half seconds.[50] De Silva's report matches Frederick's first declared length of five minutes and twenty-five seconds, but identifies the file under investigation as "SL1 Channel 4.3GP".[51] Finally, Evangelos Yfantis, a third GoSL investigator, describes analysing two videos obtained from the GoSL, one in 3GP format and a second "downloaded from an internet broadcast site."[52]

Once again, use of a cryptographic hash would have neutralized these discrepancies by establishing continuity of the evidence across sites, time, and researchers. Instead, omission of the hash serves as a procedural obfuscation that allows inconsistencies to multiply in number and consequence. Altogether, these variances erode trust both in the competence of the investigations and in the meaning of their reports.

Spivack and Fredericks further contradict each other on the number of frames in each video. Both initially identify the second, extended video as containing 2411 frames.[53] Yet, Fredericks later identifies the last image as, "Image 2410".[54] Spivack indexes the shorter video as, "frame 1–542".[55] Fredericks, on the other hand, calculates five groups of 100 frames, plus an additional group of 41 "images". If "images" and "frames" are equivalent, which he does not clarify, this would mean that, this would mean that Fredericks calculates the shorter video to contain only 541 frames. Perhaps Fredericks began his index at zero, while Spivack began his at one. While this would be a relatively simple explanation, the reader must still hypothesize a solution to the discrepancies. Although for a difference of one frame it may be tempting to discard this as a trivial mistake, any concrete discrepancies provide grounds for doubt and dispute of the whole.

Doubt about whether the GoSL and U.N. analysts actually examined the same video files pre-empts meaningful consensus among scientific experts and degrades the public credibility of the forensic investigations in general. Weak forensic credibility leaves publics more likely to ignore or confuse any and all results, and to turn to alternative sources of authority such as their own personal experience.

Proprietary Interests in Conflict with Experimental Reproducibility

Proprietary claims to investigative methods and tools also obstruct the reproducibility of the Channel 4 forensic analyses. For instance, De Silva introduces his report by declaring, "The experimental procedures used in this analysis include techniques that have been developed . . . at the University . . . . These techniques or their results may not be deployed . . . without appropriate permission."[56] The implicit suggestion is that some investigators may obtain permission, but not all. Those denied would also be denied the opportunity to scrutinize the full methodology and data behind De Silva's findings.

Subtler, yet still problematic, Spivack deploys proprietary software, Cognitech Video Investigator, in his investigation in a manner that inhibits external review. Spivack's reports include three significant obstacles to reproducibility: black-boxing technical functions, risking procedural artifacts that could obscure rather than clarify the evidence, and presenting a mediated manipulation of evidence instead of the evidence itself. As a result, the authority of his report is based in part on preclusion of counter-scrutiny rather than the accountability of scientific peer review.[57]

First, Spivack offers no explanation of how Cognitech software actually operates. He writes of one investigative action, "Cognitech VideoInvestigator (*sic*) software was used . . . apparent velocity estimation was calculated and the resulting data applied to a mosaic reconstruction utility to create a single panoramic still image from the video segment."[58] In other words, the Cognitech proprietary software pieced together a series of video frames into one composite still image, called a mosaic reconstruction. Yet none of the data produced during the intermediary step of "apparent velocity estimation" is included, nor is there any reference to a functional definition of the mosaic method applied. Absence of such documentation black-boxes technical functions and inhibits external review of the stated interpretation.

Second, vaguely-defined manipulation of the original image in this manner risks imposing artifacts and distortions on the video. These artifacts may obscure rather than enlighten the video's forensic truth-value. To his credit, Spivack warns of this risk, writing, "As a normal consequence of [the] procedures . . . visual artifacts from the image boundaries

are visible, as are variations in histogram values that present as differences in lighting and contrast in different regions of the images [Picture 1]."[59] (De Silva, using a different mosaic reconstruction function with similar risk of artifacts, gives no such warning.[60]) Had Spivack clarified the method, or even referenced a specific definition of the method, and shown a sample of the component images, a reviewer might be able to observe the effects and reason about them. Leaving an explicit trail of each step of the manipulation, documented for review, could also reduce the peril of mistaking procedural artifacts for relevant evidence. Absence of such transparency once again prohibits external scrutiny of the investigative procedure.

Third, performing the mosaic manipulation offered no clear benefits to Spivack's analysis, raising questions as to why it was done in the first place. Spivack explains that his goal for the procedure was, "to produce a still image of the individual previously described . . . as wearing a 'clean white shirt'." Following production of the composite still, he concludes, "the white shirt has visible red stains."[61] Spivack offers no further data, reasoning or opinions about this mosaic manipulation apart from reproducing the resulting image [Picture 1].[62] In other words, the sole finding he generates is that red stains are visible on the white shirt in the image.[63]

Yet, it was not necessary to perform the proprietary velocity estimation and mosaic manipulation to reach that conclusion. Fredericks reproduces in his report a single frame of video, unaltered, in which the red stains are also readily visible [Picture 2].[64] In short, the findings presented (the visibility of red stains) are disconnected from the means that supposedly achieved them — Cognitech mosaic manipulation. Proprietary software manipulations performed with neither clear benefit nor functional transparency mask the original evidence. Readers are able to reason about Spivack's mediated manipulation of the evidence, but not about the evidence itself.

Spivack offers cause for additional concern when he appropriately discloses that he is a beta-tester and technical representative for Cognitech, Inc., the company that produces and sells the software he uses to perform these mosaic reconstructions.[65] Professional conflict of interest poses a risk of bias toward applying this tool without clear benefit, and obscuring rather than illuminating the evidence.[66] Commercial interest may conflict with disclosure of methods and algorithms. In the worst-case scenario,

then, Spivack's application of Cognitech mosaic manipulations promotes marketing rather than furthering the analytic conclusions of the investigation. Moreover, there is a continuing question of conflict of interest in the emergent field of FVA more broadly, if forensic software developers accumulate uncontested authority.

Secrecy as an Obstacle to Experimental Reproducibility

The report of GoSL investigator Evangelos Yfantis provides still clearer evidence of the urgency of conflict of interest protections for FVA software developers, and the exigency of transparency in investigative methods and technologies. Yfantis wrote his own forensic software for the purposes of the Channel 4 investigation. He then deployed it with far less transparency of function and purpose than Spivack did with Cognitech mosaic reconstructions.

For example, Yfantis developed a test to compare images of blood in the Channel 4 videos with representations of blood in a reference pool of images of known violent crime scenes. First, he obtained the set of reference images from the Metropolitan Police Department in the U.S.[67] Then, he employed "self-developed in house computer software" to extract the red, green, and blue planes from a digital image.[68] Next, he measured the histogram of the red video plane, a graph of the frequency of red brightness values. The histogram shows peaks that identify the pixel brightness values that occur most often in the plane.[69] Finally, he used "mathematical computations", which he does not describe, to contrast the red histogram values of blood scenes in the two leaked videos with red histogram values of blood scenes in a series of reference crime scene photo and video images. Finding a significant difference, Yfantis deduces that blood depicted in the Channel 4 videos "is not real blood". In other words, the difference in red histogram values between the leaked videos and his reference images leads him to conclude that the Channel 4 videos depict living persons wearing fake blood.[70]

Picture 1: (Original size) Spivack presents this as "Frame 804–816 Apparent Velocity Estimation Calculated Mosaic Reconstruction".[71] *The black rectangles along the top of the image are examples of image boundary artifacts.*

Picture 2: (Original size) Fredericks reproduces a single frame in his report, in which the red stain on the white shirt is clearly visible.[72]

The investigative methods and technologies that Yfantis created and deployed lack even the most basic transparency necessary for external evaluation or experimental replication. Yfantis provides no information about the selection mechanism either for the pool of reference images, or for the individual frames of video analysed. He provides no reporting of error measurement for his self-developed software. The report fails to state the controls of the experimental measurement, and the observed measurement error under those controls.[73] In other words, readers have no way of knowing whether the measurement does in fact discriminate between real and blood substitute, or whether the software just reports measurement noise. Without this information, there is little to no opportunity for third parties to evaluate the accuracy of his techniques.

Unfortunately, the Channel 4 FVA dispute has failed to promote agreement among parties, and instead become yet another obstacle to reconciliation in post-war Sri Lanka. The lack of disclosed methods, and analytic gaps between evidence and conclusions in the FVA reports may have contributed to this outcome. That the problem of concealed methods appears in both the U.N. and GoSL FVA reports demonstrates a systematic weakness in the investigatory paradigm. Presentation of an experimental finding without explaining the mechanism by which it was achieved forces the audience into blind trust. Concealing investigative methods, and restricting access to investigative technologies, prevents others from challenging the accuracy of the results. It precludes reproducibility, and thus pre-emptively censors reasoned critique.

CONCLUSIONS

Digital video resists censorship in certain respects because it largely defies containment. In the case at hand, the Channel 4 video has been widely duplicated and broadly accessed. Yet, when the standards to authenticate it are concealed, publics are unable to know whether determinations of authenticity are incompetent.

Commitment to design and adopt open FVA tools and methods will best enable experts to contest and publics to credit online video-speech. Forensic experts should disclose a reproducible basis for each opinion. Forensic tool vendors should provide, at a minimum, a sound scientific basis for the interpretation of results. Finally, courts should have the abil-

ity to compel disclosure of investigative methods. Forensic methods of reducing video data to measurements, application of these measurements to a given case, and steps leading to conclusive opinions, should all be open to scrutiny.

Open investigative methods would facilitate a minimum level of peer-review that could help to unmask subtle defects in experiments, provide courts with newly efficient economies of scale, and further democratic legitimacy by reducing pre-emptive censorship of reasoned critique and facilitating public debate. The development of such a model of best practices would strengthen FVA standards more broadly, and enhance the ability of this emergent discipline to facilitate consensus.

In a dispute of any consequence, parties deserve the opportunity to question the methods behind expert testimony against them. In a public dispute touching post-war stability, as does the video authentication struggle in Sri Lanka, the risk of censorship through meaning-manipulation becomes greater and the need for open methods more urgent.

1 The author thanks Kiel Brennan-Marquez, Robert Crusz, Dan Kahan, Eli Omen, Lisa Larrimore Ouellette, Nagla Rizk, and Pranesh Prakash for providing generous feedback on earlier drafts.

2 *See, e.g.*, Christoph Koettle, *Can Video Document Possible War Crimes in Syria?*, WITNESS BLOG (Jan. 8, 2013), http://blog.witness.org/2013/01/video-war-crimes-in-syria/ ("What power does a Syrian cell phone video have, for justice and deception?"); Pepper Spray Incident; cf. Eric Garner video.

3 *Lanka Denies Execution Video*, BBC SINHALA (Jan. 8, 2010) http://www.bbc.co.uk/sinhala/news/story/2010/01/100108_govt_jds.shtml.

4 CHITTA RANJAN DE SILVA ET AL., REPORT OF THE COMMISSION OF INQUIRY ON LESSONS LEARNT AND RECONCILIATION 147 (2011), http://www.llrcaction.gov.lk/en/llrc-report.html [hereinafter LLRC REPORT].

5 *See generally* U.N. Special Rapporteur on Extrajudicial, Summary, or Arbitrary Executions, *Technical Note Prepared by the Special Rapporteur on Extrajudicial, Summary, or Arbitrary Executions, Philip Alston, in Relation to the Authenticity of the "Channel 4 Videotape"*, U.N. Human Rights Council, Appendix to U.N. Doc. A/HRC/14/24/Add.1 (Jan. 7, 2010) (*prepared by* Philip Alston), http://www2.ohchr.org/english/issues/executions/docs/TechnicalNoteAppendix.pdf [hereinbefore and hereinafter Alston Technical Report] (an appendix to the addendum to the Special Rapporteur's report, containing each of the opinions provided by the experts he consulted); s*ee also* U.N. SECRETARY-GENERAL'S PANEL OF EXPERTS ON ACCOUNTABILITY IN SRI LANKA, REPORT OF THE SECRETARY-GENERAL'S PANEL OF EXPERTS ON ACCOUNTABILITY IN SRI LANKA 43, note 87 (2011), http://www.un.org/News/dh/infocus/Sri_Lanka/POE_Report_Full.pdf (reporting Special Rapporteur Alston's conclusion that the forensic analyses provided "strong indications" of authenticity).

6 *See* U.S. DEPARTMENT OF STATE, FACTUAL SUPPLEMENT TO THE REPORT TO CONGRESS BY THE GOVERNMENT OF SRI LANKA AND INTERNATIONAL BODIES 15 (2012) (summarizing the U.N. and GoSL forensic findings). *See also* K.T. Rajasingham, *Video Footage Fake: Media Expert Siri Hewa Picks Up Holes in UN Rapporteur's Findings*, ASIAN TRIBUNE (June 4, 2010), http://www.asiantribune.com/news/2010/06/04/video-footage-fake-media-expert-siri-hewa-picks-holes-un-rapporteur%E2%80%99s-findings.

7 *See* U.S. DEPARTMENT OF STATE, *supra* note 6, at 16 ("The State Department is not aware of any action by the GSL . . . establishing an independent investigation into the Channel 4 videos.").

8 *See id.* at 16; *see also* LLRC REPORT, *supra* note 4, at 151 ("The Commission finds that there are troubling technical and forensic questions of a serious nature that cast significant doubts about the authenticity of this video and the credibility and reliability of its content."). *Compare* Special Rapporteur on Extrajudicial, Summary or Arbitrary Executions, *Report of the Special Rapporteur on Extrajudicial, Summary or Arbitrary Executions, Addendum: Summary of Information, Including Individual Cases, Transmitted to Governments and Replies Received*, U.N. Human Rights Council, *430, U.N. Doc. A/HRC/17/28/Add.1, (May 27, 2011) (prepared by* Christof Heyns), http://www.ohchr.org/Documents/Issues/Executions/A-HRC-17-28-Add1.pdf [hereinafter Heyns Addendum], and particularly the two reports contained in it. In the Heyns Addendum, two of the reports included relate to forensic analysis of the Channel 4 video. Jeff S. Spivack, Forensic Video Analysis Supplemental Report Re: Authenticity of Digital

Video/Audio Recording of Purported Sri Lanka Executions, *in* Heyns Addendum, at 430 (finding the video to be authentic) [hereinafter Spivack FVA Supplemental Report for Heyns]; Grant Fredericks, *Report Of Mr. Grant Fredericks, A Forensic Video Analyst*, *in* Heyns, Addendum, at 450 (also finding the video to be authentic) [hereinafter Fredericks FVA Report for Heyns]; A.A.M. Nizan, *Forensic Expert on Digital Video Proves Channel 4 Video on Sri Lanka as a Fake*, ASIAN TRIBUNE, June 16, 2011, *available at* http://www.asiantribune.com/news/2011/06/16/forensic-expert-digital-video-proves-channel-4-video-sri-lanka-fake, *and* Hassina Leelarathna, *UN Officials' Channel 4 Video Analysis 'Forensic Hoax'*, UPDATES: SRI LANKA USA, http://srilankausa.weebly.com/un--forensics-hoax.html.

9 Dr. Murphey is a research scientist in computer forensics who consults on multimedia and video forensics. Rich Murphey, Electrical and Computer Engineering, http://murphey.org/ (Dr. Murphey "provide[s] advanced analysis services in Computer Forensics ... Multimedia Forensics (audio/video/images) ... [and conducts] basic research in forensic sciences.").

10 *See generally*, Thomas I. Emerson, *The Doctrine of Prior Restraint*, 20 LAW & CONTEMP. PROBS. 648 (1955) (analyzing the concept and doctrine of prior restraint).

11 *See, e.g.*, Jack Balkin, *Old-School/New-School Speech Regulation*, 127 HARV. L. REV. 2296 (2014) ("[T]he infrastructure of free expression . . . largely held in private hands, is the central battleground over free speech in the digital era."). For an analysis of the First Amendment and state influence over information intermediaries, see Jack Balkin's theory of "collateral censorship" in *Free Speech and Hostile Environments*, 99. COLUM. L. REV. 2295 (1999).

12 Lawrence Lessig pointed out this phenomenon both well and early. *See, e.g.*, Lawrence Lessig, *What Things Regulate Speech: CDA 2.0 vs. Filtering*, 38 JURIMETRICS J. 629 (1998) (predicting in 1998 that Internet filtration technologies that enable upstream control would facilitate state censorship); LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE (1999). For another early and influential articulation of a similar argument, see James Boyle, *Foucault in Cyberspace: Surveillance, Sovereignty, and Hardwired Censors*, 66 U. CIN. L. REV. 177 (1997).

13 *See generally* Jack Balkin, *Old-School/New-School Speech Regulation*, 127 HARV. L. REV. 2296 (2014); (Yale Law School Public Law Research Paper No. 491), *available at* http://harvardlawreview.org/2014/06/old-schoolnew-school-speech-regulation/ (discussing *ex ante* state regulation of speech in a digital world).

14 Marvin Ammori, *The 'New' New York Times: Free Speech Lawyering in the Age of Google and Twitter*, 127 HARV. L. REV. 2259, 2273 (2014) ("Today's speech lawyers craft speech rules for the millions of users speaking through their sites and adopt strategies to implement them in the hard cases. These lawyers effectively engage in private speech rulemaking, adjudication, and enforcement.").

15 Mark Tushnet, *Introduction: Reflections on the First Amendment and the Information Economy*, 127 HARV. L. REV. 2234, 2256-57 (2014) ("With the state action doctrine in hand, we could call [collateral censorship by Internet intermediaries] simply censorship and ask whether the censorship could be justified.").

16 For a similar argument in the context of network neutrality under the Indian constitutional guarantee of free speech, see GAUTAM BHATIA, OFFEND SHOCK OR DISTURB: FREE SPEECH UNDER THE INDIAN CONSTITUTION, ch. 12 (OUP 2015: Forthcoming).

17 *See generally* HARRY COLLINS, CHANGING ORDER: REPLICATION AND INDUCTION IN SCIENTIFIC PRACTICE (1992).

18 In an early precursor to crowd sourcing during the seventeenth century, European scientists began to report rich circumstantial details to encourage readers to envision and explicate experimental scenes that they did not directly observe. *See* Steven Shapin, *Pump and Circumstance: Robert Boyle's Literary Technology*, 14 SOC. STUD. SCI. 481, 483 (1984) ("Boyle proposed that matters of fact be generated by a multiplication of the witnessing experience."). Historians Steven Shapin and Simon Schaffer have termed this process, "virtual witnessing." STEVEN SHAPIN & SIMON SCHAFFER, LEVIATHAN AND THE AIR-PUMP: HOBBES, BOYLE, AND THE EXPERIMENTAL LIFE 60 (1985). Within that model, "the constitution of matters of fact," they point out, "involved the multiplication of witnesses." *Id.* at 20. Rhetorical strategies of hyper-detailed experimental reporting thus aimed to draw readers into a participatory production of fact-based consensus. *See generally* Richard Cunningham, *Virtual Witnessing*, 34 PHIL. & RHETORIC 207 (2001); *see also* Simon Schaffer, *Self-Evidence*, 18 CRITICAL INQUIRY 327, 330 (1992) (noting that through this participatory process, science acquired the "public warrant of collective authority").

19 *See, e.g.,* Simone Milani et al., *An Overview on Video Forensics*, 1 APSIPA TRANSACTIONS ON SIGNAL & INFO. PROCESSING, 1 (e2 doi:10.1017/ATSIP.2012.2, 1, 2012); Hany Farid, *Exposing Digital Forgeries from JPEG Ghosts*, 4 IEEE TRANSACTIONS ON INFO. FORENSICS & SECURITY 154 (doi:10.1109/TIFS.2008.2012215, 2009); Babak Mahdian & Stanislav Saic, *Using Noise Inconsistencies for Blind Image Forensics, 27* IMAGE & VISION COMPUTING 2497 (doi:10.1016/j.imavis.2009.02.001, 2009); W. Sabrina Lin et al., *Digital Image Source Coder Forensics Via Intrinsic Fingerprints,* 4 IEEE TRANSACTIONS ON INFO. FORENSICS & SEC. 460 (doi:10.1109/TIFS.2009.2024715, 2009); Wiger van Houten & Zeno Geradts, *Source Video Camera Identification for Multiply Compressed Videos Originating from YouTube,* 6 DIGITAL INVESTIGATION 48 (doi:10.1016/j.diin.2009.05.003, 2009); Ghulam Muhammad et al., *Passive Copy Move Image Forgery Detection Using Undecimated Dyadic Wavelet Transform,* 9 DIGITAL INVESTIGATION 49 (doi:10.1016/j.diin.2012.04.004, 2012); Alan J. Cooper, *Improved Photo Response Non-Uniformity (PRNU) Based Source Camera Identification,* 226 FORENSIC SCI. INT'L 132 (doi:10.1016/j.forsciint.2012.12.018, 2013).

20 Milani et al., *supra* note 19, at 2.

21 *Id.*

22 FVA exists within a broader landscape of digital forensics that more generally lack mature standards. Recognition of the need to clarify methodological standards for digital forensics as a whole is not entirely new. The FBI formed a Scientific Working Group on Imaging Technology in 1997 with the mission of "creating standards for digital and multimedia evidence". SCIENTIFIC WORKING GROUP IMAGING TECHNOLOGY, https://www.swgit.org (last visited Feb. 8, 2014). But a decade later, doubts remained as to the strength of these standards. Law Professor Erin Murphy warned in 2007 against overconfidence in emergent forensics technologies, suggesting that "false certainty" regarding these techniques might "exacerbate the conditions that first caused forensic sciences to fall into disrepute." Erin Murphy, *The New Forensics: Criminal Justice, False Certainty, and the Second Generation of Scientific Evidence*, 95 CALIF. L. REV. 721, 721–2 (2007). Two years later, in 2009, the National Research Council reported of digital forensics as a whole, "the digital evidence community does not have an

agreed certification program or list of qualifications." NATIONAL RESEARCH COUNCIL, STRENGTHENING FORENSIC SCIENCE IN THE UNITED STATES: A PATH FORWARD 181 (2009). And again, in 2011, forensic computing engineers Jason Beckett and Jill Slay called for "criteria to assess digital forensics as a science". Jason Beckett & Jill Slay, *Scientific Underpinnings and Background to Standards and Accreditation in Digital Forensics*, 8 DIGITAL INVESTIGATION 114, 114 (2011). For recent technical overviews of the field of FVA, see Milani et al., *supra* note 19; *see also* Babak Mahdian et al., *A Bibliography on Blind Methods for Identifying Image Forgery,* 25 SIGNAL PROCESSING: IMAGE COMM. 389 (doi:10.1016/j.image.2010.05.003, 2010); Hany Farid, *Image Forgery Detection: A Survey*, 26 IEEE SIGNAL PROCESSING MAG. 16 (doi:10.1109/MSP.2008.931079, 2008).

23 *See generally* Sheila Jasanoff, *The Eye of Everyman: Witnessing DNA in the Simpson Trial,* 28 SOC. STUD. SCI. 713 (1998).

24 *See, e.g.*, ANN MARIE LIPINSKI ET AL., TRUTH IN THE AGE OF SOCIAL MEDIA (2012) (a report for the Nieman Foundation for Journalism, looking at how the BBC, the AP, CNN, and other news organizations are addressing questions of truth and verification); *Arab Spring Leads Surge in Events Captured on Cameraphones*, THE GUARDIAN (Dec. 29, 2011), http://www.theguardian.com/world/2011/dec/29/arab-spring-captured-on-cameraphones; Kate Bulkley, *The Rise of Citizen Journalism*, THE GUARDIAN (Jun. 10, 2012), http://www.theguardian.com/media/2012/jun/11/rise-of-citizen-journalism.

25 For instance, Derek Bousé argues that most wildlife films operate according to formal dramatic conventions, rather than scientific criteria, because the neutral objectivity that is the goal of scientific observation would never survive the ratings-driven television market. Yet, Bousé also points out that filmmakers conceal this fact in order to achieve documentary appeal. Derek Bousé, *False Intimacy: Close-Ups and Viewer Involvement in Wildlife Films*, 18 VISUAL STUD. 123 (2003).

26 *Id.* at 22.

27 Sheila Jasanoff, *Transparency in Public Science*, 69 LAW & CONTEMP. PROBS. 21, 21 (2006), *available at* http://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=1385&context=lcp.

28 Matthew Weaver & Gethin Chamberlain, *Sri Lanka Declares End to War with Tamil Tigers*, GUARDIAN (May 19, 2009), http://www.theguardian.com/world/2009/may/18/tamil-tigers-killed-sri-lanka.

29 *See, e.g., Foreign Terrorist Organizations*, U.S. DEPARTMENT OF STATE, http://www.state.gov/j/ct/rls/other/des/123085.htm (last visited Aug. 10, 2014); *EU Says Tamil Tigers 'Terrorists'*, BBC NEWS (May 29, 2006), http://news.bbc.co.uk/2/hi/south_asia/5028384.stm; *Indian Court Upholds LTTE Ban*, BBC SINHALA (Nov. 11, 2008), http://www.bbc.co.uk/sinhala/news/story/2008/11/081111_india_ltte.shtml; *Proscribed Terrorist Groups*, U.K. HOME OFFICE (Dec. 13, 2013), https://www.gov.uk/government/publications/proscribed-terror-groups-or-organisations--2; *Listed Terrorist Entities*, Public Safety Canada, http://www.publicsafety.gc.ca/cnt/ntnl-scrt/cntr-trrrsm/lstd-ntts/crrnt-lstd-ntts-eng.aspx; *LTTE is Banned by the SL Govt*, MINISTRY OF DEFENCE, SRI LANKA (Dec. 30, 2010), http://www.defence.lk/new.asp?fname=20090107_15.

30 Jon Lee Anderson, *Death of the Tiger*, NEW YORKER, Jan. 17, 2011, at 41, *available at* http://www.newyorker.com/magazine/2011/01/17/death-of-the-tiger.

31 *Sri Lanka Steps Up Death Video Rebuttal*, CHANNEL 4 NEWS (Sep. 11, 2009), http://www.channel4.com/news/articles/politics/international_politics/sri%2Blanka%2Bsteps%2Bup%2Bdeath%2Bvideo%2Brebuttal/3340612.html.

32 It remains difficult to seek to establish veracity of a video using blind methods that do not depend on prior knowledge of the video's source. Investigators may seek to conclusively determine whether compression artifacts, such as spatial frequencies skewed by quantization, are consistent or inconsistent with expected values. *See,* I-Chuan Chang et al., *A DCT Quantization-Based Image Authentication System for Digital Forensics,* SADFE '05: PROCEEDINGS OF THE FIRST INT'L WORKSHOP ON SYSTEMATIC APPROACHES TO DIGITAL FORENSIC ENGINEERING 223 (2005); *see also* Babak Mahdian & Stanislav Saic, *Blind Authentication Using Periodic Properties of Interpolation,* 3 IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY 529 (2008).

33 Jeff S. Spivack, *Forensic Video Analysis Report Re: Authenticity of Digital Video/Audio Recording of Purported Sri Lanka Executions*, *in* Alston, Technical Report, *infra* note 70 [hereinafter Spivack FVA Report for Alston].

34 *See* U.S. DEPARTMENT OF STATE, *supra* note 34, at 16 ("The State Department is not aware of any action by the GSL . . . establishing an independent investigation into the Channel 4 videos.").

35 *See* Lasanda Kurukulasuriya, *Channel 4 Unravelled, Lies Unpacked*, SUNDAY TIMES, Aug. 7, 2011, available at http://www.sundaytimes.lk/110807/Columns/Lasandak.html (reporting on a video produced by the GoSL in response to Channel 4, arguing that allegations of war crimes and media evidence in support were manufactured in the West), and SRI LANKA MEDIA WATCH, APPALLING JOURNALISM 23-24 (2011) (reporting that the videos may have been filmed with a video camera rather than a mobile phone, and suggesting that they may depict LTTE cadres performing executions while wearing Sri Lankan military uniforms and speaking in Tamil), available at http://www.engagesrilanka.com/mediawatch.html.

36 *See generally* The Editorial Board, *Holding Sri Lanka to Account*, N.Y. TIMES (Feb. 4, 2014), http://www.nytimes.com/2014/02/04/opinion/holding-sri-lanka-to-account.html?_r=0. *See also* PERMANENT PEOPLE'S TRIBUNAL, PEOPLES' TRIBUNAL ON SRI LANKA (2014), *available at* http://www.ptsrilanka.org/images/documents/ppt_final_report_web_en.pdf (considering both video and photographic forensic evidence, often together with eye witness accounts of torture or rape. These accounts put the forensic analysis in a broader perspective of similar events in series, which the report concludes to be state sponsored patterns of directed violence.).

37 The analysis in this Part is deeply indebted to the expert contributions of Dr. Rich Murphey.

38 Special Rapporteur on Extrajudicial, Summary, or Arbitrary Executions, *Rep. of the Special Rapporteur on Extrajudicial, Summary or Arbitrary Executions, Addendum: Communications to and from Governments*, U.N. Human Rights Council, 264–269, U.N. Doc. A/HRC/14/24/Add.1 (June 1, 2010) (*prepared by* Philip Alston), *available at* http://www2.ohchr.org/english/bodies/hrcouncil/docs/14session/A.HRC.14.24.Add1.pdf (hereinafter Alston Addendum).

39 Eventually the GoSL provided two reports that were submitted to the Commission of Inquiry on Lessons Learnt and Reconciliation (CILLR) in 2011. One report was submitted to

the CILLR on July 13, 2011. Chathura R. De Silva, *A Technical Analysis On The Channel 4 Video Footage*, *in* LLRC REPORT, *supra* note 4, at 154 [hereinafter De Silva Technical Analysis]. A second report was submitted to the CILLR on October 3, 2011. E.A. Yfantis, *A Technical Report with Analysis and Measure for the Channel 4 Videos*, *in* LLRC REPORT, *supra* note 4, at 217 [herinafter Yfantis Technical Report].

40 *See e.g.,* Vassil Roussev, *Hashing and Data Fingerprinting in Digital Forensics*, 7 IEEE SEC. & PRIV. 49 (Mar.-Apr. doi:10.1109/MSP.2009.40, 2009); Paul Owen & Paula Thomas, *An Analysis of Digital Forensic Examinations: Mobile Devices Versus Hard Disk Drives Utilizing ACPO & NIST Guidelines,* 8 DIGITAL INVESTIGATION 137 (doi:10.1016/j.diin.2011.03.002, 2011); SCIENTIFIC WORKING GROUP ON IMAGING TECHNOLOGY, SECTION 13 BEST PRACTICES FOR MAINTAINING THE INTEGRITY OF DIGITAL IMAGES AND DIGITAL VIDEO (2012), *available at* https://www.swgit.org/pdf/?docID=54.

41 *See generally,* Eric Thompson, *MD5 Collisions and the Impact on Computer Forensics*, 2 DIGITAL FORENSICS 36 (2005); *see also* Vassil Roussev et al., *md5bloom: Forensic Filesystem Hashing Revisited,* 3 DIGITAL INVESTIGATION 82 (doi:10.1016/j.diin.2006.06.012, 2006).

42 Both the U.N. and GoSL reports do make an initial assessment of the metadata annotations held in an 'outer' container of the video file format, completely separate from the 'inner' containers holding the video and audio streams. While this might appear to be a test of integrity, it is not. The reports acknowledge that the outer container metadata is easily manipulated without a trace, and thus invalid for the purpose of any conclusive interpretation of video data properties, and not a substitute for the hash function. *See, e.g.*, Spivack, FVA Report for Alston, *supra* note 33, at 9 ("It is theoretically possible to alter or delete metadata in a multimedia file, so the metadata contained in the file submitted for analysis cannot be considered absolutely conclusive with respect to accuracy or containing all possible file attributes.").

43 Jeff Spivack, telephone communication with author Rebecca Wexler, Jan. 2013.

44 In the first round of reports on the initial, shorter video, U.N. investigator Grant Fredericks analysed a one minute seventeen second file named "massacrevideo.3gp", sourced to a London Times reporter. Fredericks FVA Report for Heyns, *supra* note 8, at 451. Yet Journalists for Democracy in Sri Lanka (JDS), the earliest known source in the chain of custody, provided the authors with a one minute seventeen second video named "VideoDJ.3GP." JDS assured the author that this file is "exactly the same original file received from Sri Lanka", and maintains that the original video was in 3GP format. Bashana Abeywardane, JDS convener, email communication with author Rebecca Wexler, Feb. 22, 2013. "VideoDJ.3GP" is also the name of the file that U.N. investigator Jeff Spivack examined, sourced to JDS via the U.N. Spivack, FVA Report for Alston, *supra* note 33, at 2. Yet, GoSL investigator Siri Hewawitharana analysed an AVI and QuickTime formatted video of slightly over one minute two seconds. Alston Addendum, *supra* note 38, at 268. GoSL investigator Chathura De Silva analysed a video of one minute twenty-five seconds. De Silva Technical Analysis, *supra* note 39, at 157.

45 De Silva Technical Analysis, *supra* note 39, at 157.

46 Heyns Addendum, *supra* note 8, at 425.

47 Spivack FVA Supplemental Report for Heyns, *supra* note 8, at 430.

48 Fredericks FVA Report for Heyns, *supra* note 8, at 451.

49 *Id.* at 453.

50 *Id*.

51 De Silva Technical Analysis, *supra* note 39, at 159–60.

52 *Id.*

53 Spivack writes, "Frame by frame analysis of the 2411 video frames for content was conducted using Cognitech Video Investigator and Elecard StreamEye." Spivack FVA Supplemental Report for Heyns, *supra* note 8, at 434. Fredericks concurs that the extended video contains 2411 frames. Fredericks FVA Report for Heyns, *supra* note 8, at 453.

54 Fredericks FVA Report for Heyns, *supra* note 8, at 470.

55 Spivack FVA Supplemental Report for Heyns, *supra* note 8, at 438.

56 De Silva Technical Analysis, *supra* note 39, at 158.

57 Crime lab forensics may prefer commercial forensic tools because they provide third party support for the credibility of methods. Yet preference for such tools also creates an incentive for investigators to fit their investigation of the data to the tool, rather than the reverse. Free/libre/open source forensic tools could help to resolve this issue by allowing investigators to customize tools to the specific problem they are investigating.

58 Spivack FVA Supplemental Report for Heyns, *supra* note 8, at 433; *see also* Spivack FVA Report for Alston, *supra* note 33, at 4 (describing his use of Cognitech's proprietary software).

59 Spivack FVA Supplemental Report for Heyns, *supra* note 8, at 434.

60 De Silva Technical Analysis, *supra* note 39, at 174.

61 Spivack FVA Supplemental Report for Heyns, *supra* note 8, at 438.

62 *Id.* at 439.

63 *Id*. at 438.

64 Fredericks FVA Report for Heyns, *supra* note 8, 460.

65 Spivack FVA Report for Alston, *supra* note 33, at 1.

66 Spivack appropriately obtained peer-review of his methodology and conclusions prior to publication, yet there are no references to any publication of the methods or algorithms applied. Further, one of the two reviewers was also an employee of Cognitech, Inc., and therefore may also have exhibited a conflict of interest. Spivack FVA Supplemental Report for Heyns, *supra* note 8, at 443.

67 Yfantis Technical Report, *supra* note 39, at 300.

68 *Id*. at 224.

69 *See generally* James Hafner, *Efficient Color Histogram Indexing for Quadratic Form Distance Functions, 17* IEEE TRANSACTIONS ON PATTERN ANALYSIS & MACHINE INTELLIGENCE *729* (1995).

70 Yfantis Technical Report, *supra* note 39, at 219.

71 *Supra* note 62.

72 *Supra* note 64.

73 *Id*.

INDIA

VISIBLE AND INVISIBLE CENSORSHIP

Pranesh Prakash

I find it a useful thought experiment to think of the number of Indians who have published in a newspaper or have had their voice or image broadcast over radio or television since India's independence in 1947, and to compare that with the number of Indians who have published on the Web since 1995, when India's first public-access Internet service provider started functioning. The latter number is surely larger. The Internet, as anyone who has ever experienced the wonder of going online would know, is a very different communications platform from any that has existed before. The medium enables those who have access to it an unprecedented ability to directly share their thoughts with millions of others in an instant, even while it replicates many of the inequities of other media.

The various kinds of state, corporate, and societal regulations and impositions that existed in pre-digital times continue to exist, albeit they have changed, though not necessarily for better. In this chapter, I hope to show the regulatory architecture of digital censorship in India. In particular, through the examples of the Intermediary Guidelines Rules, the ham-handed curbs on SMS and web pages in August 2012, arrests under the IT Act, and websites blocked under copyright enforcement, I shall make the argument that the most important safeguard against censorship is visibility and that we are fast losing that feature. The examples I explore shall demonstrate that public reaction to a censorship law depends less on how damaging it is (seen as how much speech can be curbed without sufficient justification and due process of law) and more on how direct it is and how

visible it is.

BRIEF CHRONOLOGY OF DIRECT STATE CENSORSHIP OF THE INTERNET IN INDIA

India has had censorship of the Internet since the middle of the nineteen nineties.[1] At that time the only way of accessing the Internet was through Videsh Sanchar Nigam Limited (VSNL), the state monopoly internet service provider (ISP). During this period, access to websites of certain voice-over-IP (VoIP) providers (like Vocaltec, Net2Phone, etc.) was blocked alongside VoIP itself, leading to the first case filed on Internet censorship in Indian courts, in 1998.[2] VSNL argued that it had the authority to block access to regulate Internet telephony and block access to VoIP provider websites under the Indian Telegraph Act, 1885.[3] It is unclear what statutory powers it was using to block access to the website of the hacker collective Cult of the Dead Cow in 1998,[4] or to block access to the website of one of Pakistan's leading newspapers, *Dawn,* during the Kargil war between Pakistan and India in 1999,[5] even though it denied having taken such an action.[6] In 2000, while a VSNL employee initially admitted having blocked e-mails from and to the 'Middle East Socialist Network' (MESN) mailing list,[7] in an affidavit to the court in the *Arun Mehta* case, VSNL denied ever having blocked access to the eGroups.com website (which hosted the archives of the MESN list), but noted that "in view of the problem of spamming on the internet, temporarily the e-mail operations of egroups.com was stopped," and later restored.[8]

Since 2000, the licence — provided under the Indian Telegraph Act — that ISPs in India must enter into to provide Internet services includes clauses that require the ISP to take measures to prevent "objectionable" content and "anti-national activities",[9] and take down websites that unspecified "enforcement agencies" ask them to remove.[10] The Indian Telegraph Act is still in force, and it is still unclear what provision in it empowers the government to block websites.

Information Technology Act and After

In 2000, the Information Technology Act (IT Act) was passed, primarily being a law derived from the UNCITRAL Model Law on Electronic Commerce. While it contained a provision criminalizing the electronic

publication of obscene materials,[11] it did not provide the government the power to block websites for obscenity, or for any other reason.[12] However, in 2003, the Department of Information Technology issued an executive order, citing powers under section 67 (the provision on obscenity) and section 87 (the provision on subordinate legislation), empowering the newly-created Indian Computer Emergency Response Team (CERT-In)[13] to block websites,[14] even though the statute itself didn't provide the government any such powers. Extraordinarily, the Indian government accepted as much in another gazette notification, that soon followed:

> *As already noted there is no explicit provision in the IT Act, 2000, for blocking of websites. In fact, blocking is taken to amount to censorship. Such blocking can be challenged if it amounts to restriction of freedom of speech and expression. But websites promoting hate content, slander or defamation of others, promoting gambling, promoting racism, violence and terrorism and other such material, in addition to promoting pornography, including child pornography, and violent sex can reasonably be blocked since all such websites may not claim constitutional right of free speech. Blocking of such websites may be equated to "balanced flow of information" and not censorship.*[15]

This presented a novel idea in Indian freedom of expression jurisprudence which has traditionally had an expansive view on what constitutes speech,[16] but then has at times been equally expansionary as to what kind of speech may be rightfully restricted.[17] This interpretation by the Department of Information Technology seems to indicate that there are some speech that may not count as speech itself, rather than as speech that may rightfully be restricted. Given this, they state that they do not need statutory powers to engage in blocking of websites, since blocking of websites of a certain sort does not amount to 'blocking'. As per government, it is not a matter of rightfully restricting speech — for which to be constitutionally valid, they would need statutory authority — but instead, it is a matter of promoting a "balanced flow of information"[18] — for which, seemingly, executive powers seem to suffice.

The first notable action subsequent to these notifications was when CERT-In ordered Yahoo and all Indian ISPs to block access to a mailing list with around 160 members called "Kynhun" on Yahoo Groups,[19] which was being used by the Hynniewtrep National Liberation Council, a little-

known proscribed separatist group from Meghalaya, to publish a newsletter called the *Voice*. According to one commentator, that newsletter contained articles on "how the corrupt government is building non-existent roads and public utilities (and swallowing money in the process), how this minority is being victimized and such."[20] Lacking the technical capabilities of blocking a single group, multiple ISPs blocked web access to all of Yahoo Groups instead. This made it possible to keep receiving mails from that mailing list (and other mailing lists on Yahoo Groups), but prevented all web access to Yahoo Groups. In a matter of a few weeks, the excessive blocking was rectified without any public statements by either the government or the ISPs that over-blocked.

In 2004, the U.S.-based right-wing website HinduUnity.org was blocked by Indian ISPs on orders of the Mumbai police, though at least one ISP apparently refused to, citing lack of legal authority in the Mumbai police to request such a ban.[21] In 2001, it had been dropped by its American web host due to hate speech concerns.[22] But none of these events gave rise to much mainstream media attention to Internet censorship. That happened for the first time in 2006, in the aftermath of train bombings in Mumbai, when the Department of Telecommunications issued orders to ISPs to block 17 domains and web pages.[23] The timing gave rise to many rumours about the blocks having been occasioned by the bombings. However, by going through (the non-public) list one saw that the list included mostly obscure sites: a site arguing for Dalit separatism,[24] a personal website of a right-leaning Indian American,[25] little-known right-leaning American blogs which had nothing to do with India,[26] a web-based SMS gateway service,[27] and some domains that didn't even exist on the day they were blocked,[28] amongst others. The most notable website that was included in the list was HinduUnity.org (which, as noted earlier, had already been ordered to be blocked in 2004).[29] Despite the lack of popularity or notability of those 17 sites, this secretive order was noticed by ordinary Web users because of a gigantic mistake.

Amongst the 17 sites ordered to be blocked were specific blogs and pages hosted on Blogspot.com, and Typepad.com. Instead of those particular blogs being blocked, all blogs and pages hosted on Blogspot.com, Typepad.com (and Geocities, inexplicably) were blocked. This resulted in the block being noticed by a large number of people, and garnering a larger

amount of media coverage than in the past. However, the only response of the government to the media furore was that of pinning the blame on the ISPs for over-blocking,[30] rather than seeking to justify the blocking of those 17 URLs, which contained perfectly legitimate websites that didn't seem to *prima facie* violate any Indian laws.

The next time that these issues sprang into prominence of some sort was when the website of Savitha Bhabhi, an erotic webcomic, was blocked in 2009, just before a large amendment of the IT Act came into force.[31] The anonymous UK-based author of the cartoon series outed himself and contacted lawyers in India to defend his creation, but due to pressure from his embarrassed family, he dropped the matter.

In the 2008 amendment to the IT Act (which were brought into effect in October 2009), a new provision — section 69A — was added which granted the government powers to block websites if it "is satisfied that it is necessary or expedient so to do in the interest of sovereignty and integrity of India, defence of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence relating to above".

TRANSPARENCY AROUND WEBSITE BLOCKING

In 2011, I submitted a right to information (RTI) request about what websites had been blocked since the new law came into force. The government of India's reply to this RTI request was groundbreaking in a way, since it was the first time the government had provided an official list of URLs that it had blocked in India.[32] Even the publication of this list did not result in much mainstream media coverage. All eleven blocked URLs had been ordered to be blocked by courts — constituting direct state regulation — however the courts and the attorneys had done an amazingly shoddy job: some of the URLs were for Google search results rather than the web pages themselves, the whole of the Indymedia portals for San Francisco and Arizona instead of just the pages the High Court found to be defamatory, and similarly all of Webs.com was blocked instead of a specific URL. The rationale for most of these was not clear even after circumventing the blocks and visiting those pages which continued to exist.

Later, in May 2012, the Internet collective Anonymous released a list of

URLs blocked by Reliance Communications.[33] Since none of the blocks that CERT-In has ordered has been published by them, whether in the Gazette of India or on their website, this was the first time that a list of all websites blocked in India — and not just under the IT Act, since 2008 — was available in the public domain. Going through the list the same evening they were released, I found, as alleged by Anonymous, that there were more than a dozen links — mostly alluding to the involvement of a senior Reliance official, who was then in prison, in a telecommunications spectrum corruption scandal — that were blocked if one used a Reliance Communications connection but not on other ISPs.[34] However, by the next morning those links were working on Reliance networks too. This leak, even though it was reported on a prominent independent political blog, as also a blog run by a mainstream news magazine, did not get much traction in the wider mainstream media.

Apart from detailing private censorship, that leak also made it clear that BuyDomains, Fabulous Domains and Sedo.co.uk — domain name marketplaces — were being blocked on orders of the Indian government. What is less clear is whether the government had any legal authority to do so.[35]

By far the largest category of blocked websites is entertainment and files-sharing websites. One set of those (104 domains) were blocked by an interim order of the Calcutta High Court.[36] The rest of them, however, were blocked by private requests by entertainment companies subsequent to generic "John Doe" orders from courts. There is a strong case to be made that this private extension of John Doe orders is unlawful and far beyond the scope of the orders themselves.[37] Further, even if one were to argue that they were lawful, there are numerous clear examples of indefensible overreach — where sites that are clearly not engaging in copyright infringement of music or films have been blocked.[38] Thus, it is plain to see that perfectly lawful and non-infringing websites are being censored in the guise of copyright infringement.

Importantly, these private blocks defeat currently-available means of transparency. Thanks to the Right to Information Act, 2005, the list of blocked websites under section 69A is available to the public upon request, even if the IT Act does not require proactive publication of the list, as it should. This provides the opportunity for a constant vigil against dir-

ect state-ordered censorship, even if through less-than-ideal means. However, a right to information request would not cover the sites that were blocked through private requests by entertainment companies. For access to those, we had to count on leaks to the press and civil society organizations by industry insiders and unauthorized access to ISP servers.

So far in this brief history, I've covered mostly direct state censorship, and one instance of state-allowed private censorship undertaken by some entertainment companies. In the next section, I will deal with the regulations made under the intermediary liability law in India, and focus on how those regulations greatly expand the scope of state-enabled private censorship, and undermine the possibility of challenging censorship.

INDIRECT CENSORSHIP: INTERMEDIARY LIABILITY

In India, section 79 of the IT Act is the provision that provides Internet intermediaries[39] protection from liability for their users' actions. Before the 2008 amendment, it covered "network service providers", but then was expanded and re-drafted quite extensively,[40] with the jailing of Avnish Bajaj, the CEO of Bazee.com, — for one of its users offering an illegally-obtained pornographic CD for sale — being a major impetus for the provision's amendment.

On February 7th 2011, the Department of Information Technology under the Ministry of Communications and Information Technology published draft regulations under section 70 on its website (initially titled "Information Technology (Due Diligence Observed by Intermediaries Guidelines) Rules, 2011" and "Information Technology (Guidelines for Cyber Cafe) Rules, 2011") in exercise of the powers conferred by section 87(2)(zg), IT Act, read with section 79(2). Comments were invited from the public till February 25, 2011.

The Centre for Internet and Society submitted comments noting, *inter alia*, that the proposed rules were *ultra vires* the parent statute, and that some of the provisions of the draft Intermediaries Guidelines rules were plainly unconstitutional since they enabled the government to require Internet intermediaries to remove content on grounds that were far beyond those contained in Article 19(2) of the Constitution of India,[41] while the draft Cyber Cafe rules greatly encroached upon the right to privacy.[42] At

that point, the draft of the Intermediaries Guidelines rules allowed only an "authority mandated under the law for the time being in force" to complain to intermediaries and require them to "remove access" to the offending material.

The government not only ignored the problems that were highlighted by civil society organizations, but introduced far greater ones. The final version of the Information Technology (Intermediary Guidelines) Rules (hereinafter 'Intermediary Guidelines'), which have been in effect since April 2011, give not only an "authority mandated under the law", but all "affected persons"[43] great powers to censor the Internet!

Policy Sting Operation

Since there is no reporting mechanism contained in the Intermediary Guidelines, there is no means of gathering information about the usage of the rules: no one, not even the government, knows how often the rules are being used, and what content is being removed. Given that, we at the Centre for Internet and Society decided to test the censorship powers of the new rules through a 'policy sting operation', by sending frivolous and plainly defective complaints to a number of intermediaries.[44] Six out of seven intermediaries removed content, including search results listings, on the basis of the most ridiculous complaints. The people whose content was removed were not told — none wrote to us asking why we objected to their content — nor was the general public informed that the content was removed. If we hadn't kept track, it would be as though that content never existed.[45] Yet, not only was what the Internet companies did legal under the Intermediary Guideline Rules, but if they had not, they would have lost the protection from being punished for the content put up by their users.[46]

Fundamental Problems with the Intermediary Guidelines

There are many problems with the Intermediary Guidelines, but the fundamental issues are discussed below.[47]

First, it shifts the burden for exemption from liability on to intermediaries. Until the Intermediary Guidelines were brought into force, an intermediary who fell within the ambit of section 79(2) of the IT Act did not have to engage in a positive act to be able to claim exemption from liability

for the words and deeds of their users. However, the Intermediary Guidelines require that intermediaries publish the terms of service contained in Rule 3(2) of the Guidelines, appointing a Grievance Redressal Officer as under Rule 3(11), follow reasonable security practices as required by Rule 3(8), report "cyber security incidents" to CERT-In, and perform other such acts to be able to claim the exemption from liability. This might mean that non-Indian intermediaries who fail to publish new terms of service in accordance with the Intermediary Guidelines would automatically fall afoul of the law and could be held liable for their users' actions in Indian courts.

Second, it seems to pin liability on intermediaries for failing to perform acts unrelated to liability. Many of the requirements of the Intermediary Guidelines have nothing to do with the speech or conduct that may give rise to liability. The question then arises if failure to perform them could result in exemption from liability being denied. For instance, if a web hosting company failed to follow reasonable security practices or failed to report a particular 'cyber security incident', could that result in it being liable for all the defamatory content on its servers?

Third, it denies users any chance to defend their speech. The Intermediary Guidelines require that intermediaries that receive a complaint, "shall act within thirty six hours and where applicable, work with user or owner of such information to disable such information that is in contravention of sub-rule (2)". It leaves it unclear what "where applicable" means in this case. It doesn't seem to categorically state that the complainees need to be informed about complaints that the intermediary receives, nor does it categorically state that the complainee should be provided a chance to defend against the complaint. As noted above, during our policy sting operation, we did not receive a single complaint from any of the parties that might have been affected by our complaints. It seems as though none of the intermediaries ever informed those who would be affected about our complaints. The Supreme Court of India has held, "[i]n considering the reasonableness of laws imposing restrictions on fundamental right, both the substantive and procedural aspects of the impugned law should be examined from the point of view of reasonableness and the test of reasonableness, wherever prescribed, should be applied to each individual statute impugned".[48] Given this, there is a strong argument to be made

that a system for removal of content which does not embed core principles of natural justice such as the *audi alteram partem* doctrine, would fail the reasonable test of Article 19(2).[49]

Fourth, the Intermediary Guidelines greatly expand the grounds under which content can be deemed unlawful. The prior means of blocking a website required a person to approach a statutory authority under section 69A of the IT Act citing one of six grounds, mostly to do with national security. But with the Intermediary Guidelines, there are thirty-two distinct grounds, a great many of which are not constitutionally justifiable. For instance, disparaging speech — as long as it isn't defamatory — is not unlawful in India; however the Intermediary Guidelines list that as a category of prohibited speech. Advertisements promoting gambling are not unlawful in India — indeed, various state governments regularly take out print advertisements and put up billboards about their lottery schemes — but now all Internet intermediaries are required to remove content that are about gambling, even if it doesn't promote it.

Fifth, the Intermediary Guidelines make the intermediaries the judge of whether any particular content is in compliance with the law or not, rather than a judicial, or even quasi-judicial, body. This relegates speech regulation to private actors. While speech regulation by private actors isn't in itself harmful (just as speech regulation by the state by itself isn't), private actors are generally subject to far less accountability than the state.

Sixth, the law promotes a complete lack of transparency and accountability. No public notice is required to be provided that content has been removed, nor is there any reporting mechanism provided for the government to gather information about requests from intermediaries. So even the government does not know how many requests have been made after these Guidelines have come into effect, nor what content has been removed subsequent to those requests. This means that even the RTI Act, which has proven a powerful transparency tool to pry open the government, cannot be used. It also means that even the government doesn't have the information necessary to judge the law's successes and failings. In essence, this allows for invisible censorship.[50]

In the Centre for Internet and Society's proposed alternative to the government's Intermediary Guidelines, we suggest that the government

run an open and central takedown request monitoring system similar to the Chilling Effects Clearinghouse,[51] to which all those who receive notices — under the notice-and-notice provisions we've advanced — would be required to contribute.[52]

Seventh, the differentiations between categories of intermediaries is removed. A one-size-fits-all system is followed where an e-mail provider is equated with an online newspaper, which is equated with a video upload site, which is equated with a search engine: they all have to include Rule 3(2) of the Intermediary Guidelines and its thirty-two speech restrictions in their terms of service, and they will all lose exemption from liability if they fail to comply. This is like equating the post office and a book publisher as being equivalent in terms of liability for, say, defamatory speech. This is violative of Article 14 of the Constitution, which requires that unequals not be treated equally by the law.[53]

Eighth, the Intermediary Guidelines don't require a proportionality test. A DNS provider is an intermediary who can be asked to 'disable access' to a website on the basis of a single page, even though the rest of the site has nothing objectionable. Given the way the DNS system works, it is not possible for a DNS provider to selectively prohibit access to a single page. However, there is nothing in the law that would prevent such an abuse, or require the hosting provider to be contacted instead of the DNS provider in such a case.

Ninth, the Intermediary Guidelines seem to be based on a presumption of illegality of content where any allegation of unlawful content is sufficient to constitute "actual knowledge" of the content's unlawfulness.[54] In a case on defamation, the Delhi High Court held, "Rule 3(4) of the said rule provides obligation of an intermediary to remove such defamatory content within 36 hours from receipt of actual knowledge."[55] In that case the complaint to the website (Hubpages.com) contained allegations of defamation, but those allegations were held to be sufficient to constitute "actual knowledge" on the part of the website of defamation. If the Court's interpretation is correct, the Guidelines are based on the presumption that all complaints (and resultant mandatory taking down of the content) are correct, and that the incorrectness of the takedowns can be disputed in court if the complainee ever discovers that her content has been removed/blocked, etc.[56] While this was at one point the interpretation of

the Department of Electronics and Information Technology, it no longer is.[57]

Tenth, the Intermediary Guidelines are atemporal, assuming that any content removal / block has to last forever. On the other hand, many blocks, such as those relating to copyright infringement of a sporting event, are temporal in nature. Material removed or blocked due to a temporal event end up becoming permanent.

Eleventh, governmental diktat cannot just mirror industry "best practices" without any regard to constitutional validity. The Indian government has justified the Intermediary Guidelines as, "best practices followed internationally by well-known mega corporations operating on the Internet."[58] However, that ignores the fact that speech restrictions that may be imposed by "well-known mega corporations" aren't restricted by the Indian Constitution in the same manner as it restricts the actions of the government. Further, it ignores the fact that different corporations choose to have widely differing terms of service. Even different services provided by a single corporation may have different policies on what is acceptable on that platform.[59] The Intermediary Guidelines homogenizes those terms of service and makes it mandatory upon all intermediaries to include the government-prescribed terms, regardless of the services they provide and regardless of what the intermediaries consider as acceptable speech.

Twelfth, the Intermediary Guidelines do not bar governmental actors from using it to send takedown requests. Previously governmental actors would have to comply with the requirments of section 69A of the IT Act, or approach the courts — which seemingly are bound by no limits in terms of ordering the blocking of websites. Now, if they so choose, governmental actors can choose to go for the notice-and-takedown route which provides them far greater leeway — including the ability to block content it would be unconstitutional for the government to directly block under section 69A — while also providing statutory sanctions against intermediaries who fail to comply. This means that the government can get far more material removed without turning up in transparency reports of the kind that Google, Twitter, Yahoo, Facebook, and others issue.

And lastly, there are no penalties for filing frivolous complaints of the sort that we at the Centre for Internet and Society filed, nor for filing mali-

cious complaints. This creates a perverse incentive structure that privileges complainants over complainees — who aren't even required to be told about the complaints, and are not required to be afforded a chance to defend themselves.

In 1984, the then-Prime Minister of India, Indira Gandhi, was forced to sue Salman Rushdie for defamation in a London court in order to ensure one sentence was expurgated from his novel *Midnight's Children*. Today Gandhi wouldn't need to win a lawsuit against publishers. She would merely have to send a complaint to websites selling the book and it would be removed from sale unless the website wants to waive its exemption from liability.

What is astounding is not that such badly drafted subordinate legislation could be put forward by the government; it is that it could be passed despite cogent and trenchant criticism being provided as part of the public consultation process, as well as those criticisms being aired prominently in newspaper op-eds and editorials.

CONCLUSION

While the concerns with the Intermediary Guidelines were covered by the press, they mostly ignored the nuances involved in it — such as the fact that it did not require the complainee to be told, that it could lead to undetectable and invisible censorship, and other such procedural matters.[60] By contrast, the publicity provided to instances of direct state censorship has been far greater. The four instances where the press provided the most coverage for Internet censorship over the past few years were instances of direct state censorship, state-directed private censorship, and state-enabled private censorship.

Example 1: In December 2011, the Minister for Communications and Information Technology told Indiatimes, Google, Yahoo, Facebook, and Microsoft, in closed-door meetings that they should come up with a code of self-regulation using which they should pre-screen certain kinds of objectionable content, noting that the government would come up with a 'self-regulation' code for them if they didn't do so on their own.[61] This was leaked to the New York Times, and that led to constant coverage that month.[62]

Example 2: In December 2011, a journalist named Vinay Rai filed a criminal complaint against Google, Yahoo, Microsoft, and a number of other companies for hosting content that "promoted enmity between communities", as well as for hosting obscene content,[63] while former journalist named Aijaz Ashraf Qasmi filed a civil lawsuit against them. These two court cases, following soon on the heels of the government's attempts to muzzle those companies, allegedly for similar kinds of content, led to a great deal of mainstream media coverage.[64]

Example 3: In the aftermath of the violence that erupted in southern Assam in July and August 2012,[65] and a rumour-fuelled panic that spread in Bangalore and elsewhere as to the physical safety of residents from the north-east of India,[66] the government of India placed curbs on SMSes, and over a period of four days ordered 309 specific items (those being URLs, Twitter accounts, HTML tags,[67] blog posts, blogs, and a handful of websites) to be blocked.[68] This was the first time that such a large number of websites and web pages were ordered to be blocked by the government, and this led to plenty of mainstream news media coverage.

Example 4: In September 2012, a little-known cartoonist named Aseem Trivedi was charged under multiple statutes, including under section 66A of the IT Act, and arrested, followed two months later by the arrest of two girls from Mumbai for posting and 'liking' a comment on Facebook about the city-wide *bandh* (general strike) observed in Mumbai after the politician Bal Thackeray's death.[69] These outrageous arrests in September and November 2012 led to widespread condemnation of section 66A of the IT Act, which penalizes the sending of offensive messages through communication services.[70]

Instances of state-directed censorship, like those mentioned above, which can be observed much more easily, and conform to more traditional ideas of what constitutes censorship, get a fair amount of media coverage than state-enabled private censorship through the Intermediary Guidelines or through copyright infringement claims by entertainment companies, though in actuality the latter might be far more widespread than the former and affect much greater amounts of speech, and may affect far greater range of speech.

While private actors have always been involved in speech regulation,

the centrality of the role that they now occupy is something new, but is also inevitable. Those who believe that all speech regulation must be done by the state, following due process, are trying to prop up the procedural standards of a bygone world. Instead of harking back to the procedures that exist for censorship of books, and demanding that they be followed in all cases of online content, we must find new ways of countering the complete lack of transparency and accountability of private actors. We must find a way to appropriately extend the civil and political rights we enjoy against the state — which were writ when the state was the predominant actor in the silencing of speech — to act as guarantees against certain kinds of private action as well. And central to that endeavour would be the shining of light and removing the cloak of invisibility under which most forms of private censorship, whether conducted at the behest of governments, subsequent to enabling laws, or otherwise, occur. Not doing so immediately will undoubtedly make it more difficult to counter this brave new world of invisible censorship that we are transitioning into.

1 The most detailed overview of this history is presented in a monograph produced by Raman Jit Singh Chima as part of his Sarai fellowship. RAMAN JIT SINGH CHIMA, THE REGULATION OF THE INTERNET WITH RELATION TO SPEECH AND EXPRESSION BY THE INDIAN STATE (2008), http://dx.doi.org/10.2139/ssrn.1237262. For a shorter history, see Shivam Vij, *Internet Censorship in India Has a Long, Murky Past*, SUNDAY GUARDIAN (Dec. 11, 2011), http://www.sunday-guardian.com/technologic/internet-censorship-in-india-has-a-long-murky-past.

2 Arun Mehta v. Videsh Sanchar Nigam Ltd., Writ Petition (Civil) No. 4732 of 1998 (New Delhi), on file with the author.

3 Arun Mehta, *Status of VSNL Censorship of IP-Telephony Sites*, INDIA GII, http://members.tripod.com/~india_gii/statusof.htm (last updated Aug. 9, 2001), *archived at* https://archive.today/8LJqQ.

4 *Id*.

5 Siddharth Varadarajan, *Dawn Website Blocked as VSNL Plays Big Brother*, TIMES OF INDIA (July 3, 1999), *available at* http://svaradarajan.com/1999/07/03/dawn-website-blocked-as-vsnl-plays-big-brother/.

6 An erstwhile employee of Satyam Infoway, India's first private ISP, told me that the *Dawn* incident was merely one that was highly visible and hence reported in the press. He told me that Satyam Infoway would receive numerous requests — mostly unofficial and unrecorded — that would come from the Department of Telecommunication in those days, leading to websites being blocked without the press finding out.

7 Seema Kazi, the VSNL subscriber who brought this to light, noted that she, a Muslim, was told by a VSNL manager that this step was taken because "[m]uslims have links with Pakistan and because of reasons of security". Seema Kazi, Letter to the Editor, *Covert Censorship*, HINDU (Nov. 11, 2000), http://www.thehindu.com/2000/11/11/stories/05111305.htm.

8 *See* VSNL Further Aff. ¶6, in Arun Mehta v. Videsh Sanchar Nigam Ltd., *available at* https://docs.google.com/View?docid=dc72g763_15d4hj95

9 The clause covering this in various licence agreements and "guidelines" covering different actors is different, and has also varied across time. I know of no comprehensive analysis of these licences as they pertain to freedom of speech and surveillance. The licence for 'Internet service (Including Internet Telephony)' as on April 19, 2002 included these clauses:

> *1.12.09. The [licensee] shall ensure that objectionable, obscene, unauthorised or any other content, messages or communications infringing copyright, [i]ntellectual property right and international & domestic cyber laws, in any form or inconsistent with the laws of India, are not carried in his network, the ISP should take all necessary measures to prevent it. In particular, [the licensee] is obliged to provide, without delay, all the tracing facilities of the nuisance[-causing] or malicious messages or communications transported through [its] equipment and network, to authorised officers of [the] Government of India/State Government, when such information is required for investigations of crimes or in the interest of national security. The licence shall be governed by the provisions of the Information Technology (IT) Act 2000, as modified from time to time. Any damages arising out of default on the part of licensee in this respect shall be sole responsibility of the licensee.*
>
> *1.12.10. The use of the network for anti-national activities would be construed as an offence*

> *punishable under the Indian Penal Code or other applicable law. The networks cannot be used in such a manner as to endanger or make vulnerable [] networked infrastructure. Acts such as break-ins or attempted break-ins of Indian networks shall be regarded as an anti-national act and shall be dealt with in accordance with the Indian Penal Code. ISPs must ensure that their services are not used for such purposes.*

Licence Agreement for Provision of Internet Service (Including Internet Telephony), DEP'T OF TELECOMM. (April 19, 2002), http://dot.gov.in/sites/default/files/internet_telephony_lce.doc. Nearly identical clauses are found in the 2007 licence as well. *Licence Agreement for Provision of Internet Services*, DEP'T OF TELECOMM. (Oct. 16, 2007), http://dot.gov.in/sites/default/files/internet-licence-dated%2016-10-2007_0.pdf [hereinafter *2007 ISP Licence*].

Clause 27 of the 2007 Internet Service Guideline document, which formed the basis for the 2007 ISP licence, clarifies:

> *Flow of obscene, objectionable, unauthorised or any other content infringing copy-rights, intellectual property right and international & domestic [c]yber laws in any form over the ISP's network is not permitted and the ISP is supposed to take such measures as to prevent it. Any damages/claim arising out of default on the part of the licensee in this respect shall be the sole responsibility of the licensee.*

This pinning of liability in the licence terms is in direct opposition with the exemption from liability contained in section 79 of the IT Act. This is just one of the numerous instances of lack of coherence — and outright contradictions — in Indian information and telecommunications policy and law.

10 Clause 33.3, *2007 ISP Licence*, *supra* note 9, states:

> *The LICENSEE shall take necessary measures to prevent objectionable, obscene, unauthorized or any other content, messages or communications infringing copyright, intellectual property etc., in any form, from being carried on his network, consistent with the established laws of the country. Once specific instances of such infringement are reported to the [licensee] by the enforcement agencies, the [licensee] shall ensure that the carriage of such material on [its] network is prevented immediately.*

11 Information Technology Act, 2000, Section 67.

12 This contrasts with the way section 95 of India's Code of Criminal Procedure provides for the seizure of books declared to be punishable under sections 124A, 153A, 153B, 292, 293, and 295A of the Indian Penal Code.

13 Computer Emergency Response Teams are groups that handle computer security breaches, and the Indian CERT [hereinafter CERT-In] describes itself as the "national nodal agency for responding to computer security incidents as and when they occur." INDIAN COMPUTER EMERGENCY RESPONSE TEAM, http://www.cert-in.org.in/ (last visited Dec. 28, 2014).

14 The Gazette of India Extraordinary Part II – Section 3(i), Notification no. GSR. 181(E), Ministry of Communications and Information Technology (Department of Information Technology) – Government of India, Feb. 27, 2003, *available at* http://deity.gov.in/content/it-act-notification-no-181 (last visited Jan. 14, 2014). This was rescinded in May 2010 by another notification, after provisions on website blocking were introduced into the statute. The Gazette of India Extraordinary Part II – Section 3(i), Notification no. G.S.R. 410(E), Ministry of Commu-

nications and Information Technology (Department of Information Technology) – Government of India, May 17, 2010, *available at* http://www.egazette.nic.in/WriteReadData/2010/E_257_2011_010.pdf.

15 The Gazette of India Extraordinary Part II – Section 3(i), Notification no. G.S.R. 529(E), Ministry of Communications and Information Technology (Department of Information Technology) – Government of India, July 7, 2003.

16 *See, e.g.,* Bennett Coleman v. Union of India, (1972) 2 SCC 788 (holding that restrictions on newsprint constituted a restriction on freedom of expression, and that the right to receive information is part of the right to freedom of speech and expression). *Compare* Sec'y, Min. of Info. & Broadcasting v. Cricket Ass'n, (1995) 2 SCC 161 (holding that scarcity of spectrum does means the government has to act as a 'custodian' of the airwaves and must act in the public interest). It is instructive to note the contrast between the Supreme Court's decisions that scarcity of foreign exchange and newsprint cannot lead to greater government regulation of speech via newspapers, while also ruling that scarcity of spectrum may legitimately lead to increased government regulation of the airwaves.

17 Article 19(2) of the Constitution provides for the exceptions to the right to freedom of speech and expression enshrined in Article 19(1)(a). Post two amendments in 1951 and 1963, Article 19(2) states:

> *Article 19(2) — Nothing in sub clause (a) of clause (1) shall affect the operation of any existing law, or prevent the State from making any law, in so far as such law imposes reasonable restrictions on the exercise of the right conferred by the said sub clause in the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality or in relation to contempt of court, defamation or incitement to an offence.*

The Supreme Court has sometimes been very inconsistent in its application of Article 19(2): sometimes being very strict in its interpretation and sometimes loose. This is perhaps inevitable given the fact that the Indian Supreme Court hardly ever sits *en banc*, and this has caused many problems. *See* T.R. Andhyarujina, *Restoring the Supreme Court's Exclusivity*, HINDU (Aug. 31, 2013), http://www.thehindu.com/todays-paper/tp-opinion/restoring-the-supreme-courts-exclusivity/article5077644.ece ("With the increasing load of appeals from High Court decisions the number of judges have had to be increased periodically from eight judges in 1950 when the Constitution came into force to 31 in 2008. Presently, the Supreme Court is composed of one bench of the Chief Justice's Court of three judges and 13 or 14 benches of two judges in 13 or 14 courtrooms sitting regularly day after day. In no Supreme Court of other jurisdictions are there benches of 13 to 14 courts of two judges each as the Indian Supreme Court now has."); *see also* T.R. Andhyarujina, *Studying the U.S. Supreme Court's Working,* (1994) 4 S.C.C. J. 1, *available at* http://www.ebc-india.com/lawyer/articles/94v4a1.htm. Traditionally, the Supreme Court has been seen as the bulwark of protection against governmental encroachment into fundamental rights, while the lower courts, including sometimes the High Courts (which are also constitutional courts, and have the power of judicial review of legislation), have not always enjoyed the same reputation.

18 Notification GSR181(E), *supra* note 15.

19 *See* Ministry of Communications and Information Technology, *Blocking of Website*, PRESS INFO. BUREAU (Sept. 22, 2003), http://pib.nic.in/archieve/lreleng/lyr2003/rsep2003/22092003/

r22092003l4.html; *see also Yahoo! Groups Blocked in India*, SUN. MORNING HERALD (Sep. 26, 2003), http://www.smh.com.au/articles/2003/09/26/1064083178553.html.

20 Suresh Ramasubramanian, *Re: Dishnet Blocking Yahoogroups – More*, INDIA-GII MAILING LIST (Sept. 20, 2003, 04:39), http://permalink.gmane.org/gmane.org.telecom.india-gii/2863.

21 CHIMA, supra note 1, at 54.

22 Dean A. Murphy, *Two Unlikely Allies Come Together in Fight Against Muslims*, N.Y. TIMES (June 2, 2001), http://www.nytimes.com/2001/06/02/nyregion/two-unlikely-allies-come-together-in-fight-against-muslims.html.

23 *Directions to Block Internet Websites*, DEP'T OF TELECOMM. (July 13, 2006), *available at* https://www.flickr.com/photos/22315040@N05/15091167867/.

24 http://www.dalitstan.org.

25 http://rahulyadav.com.

26 http://princesskimberly.blogspot.com, http://mypetjawa.mu.nu, http://pajamaeditors.blogspot.com, http://exposingtheleft.blogspot.com, http://www.thepiratescove.us, http://www.bamapachyderm.com, http://merrimusings.typepad.com, and http://mackers-world.com.

27 http://www.clickatell.com

28 http://www.nndh.com and http://imamali8.com.

29 Vij, supra note 1.

30 Ministry of Communications & Information Technology, *DoT Orders Internet Service Providers to Block Only the Specified Webpages/Websites*, PRESS INFO. BUREAU (July 20, 2006), http://pib.nic.in/newsite/erelease.aspx?relid=18954.

31 Venkatesan Vembu, *Save Our Savitha Bhabhi*, DNA (July 3, 2009), http://www.dnaindia.com/analysis/column-save-our-savita-bhabhi-1270664.

32 Pranesh Prakash, *DIT's Response to RTI on Website Blocking*, CENTRE FOR INTERNET AND SOCIETY (Apr. 07, 2011), http://cis-india.org/internet-governance/blog/rti-response-dit-blocking.

33 Isac, *List of URLs Blocked by Reliance Infocomm*, ANONYMOUS (May 25, 2012), http://pastehtml.com/view/bywiha3f9.txt, *archived at* https://archive.today/Is7Sn.

34 I tried three ISPs: BSNL, Tata Indicom, and ACT Broadband.

35 Smitha Krishna Prasad, *DoT Blocks Domain Sites — But Reasons and Authority Unclear*, CENTRE FOR INTERNET AND SOCIETY (Nov 21, 2012), http://cis-india.org/internet-governance/blog/dot-blocks-domain-sites.

36 Nikhil Pahwa, *List of 104 Music Sites That The Indian Music Industry Wants Blocked*, MEDIANAMA (Mar. 15, 2012), http://www.medianama.com/2012/03/223-list-of-104-music-sites-that-the-indian-music-industry-wants-blocked/

37 *See* Ananth Padmanabhan, *Can Judges Order ISPs to Block Websites for Copyright Infringement? (Part 1)*, CENTRE FOR INTERNET AND SOCIETY (Jan. 30, 2014), http://cis-india.org/a2k/blog/john-doe-orders-isp-blocking-websites-copyright-1.

38 Sites like Pastebin.com (which only hosts text content, not audio), and sites which have content that goes far beyond the limited copyright infringing material they may have, like

Vimeo.com (a general video-hosting website) and Chakpak.com (a general entertianment website), have also been blocked.

39 The term "intermediary" is very broadly defined in s.2(w) of the IT Act: "'intermediary' with respect to any particular electronic records, means any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and includes telecommunications service providers, network service providers, internet service providers, web-hosting service providers, search engines, online payment sites, online-auction sites, online-market places and cyber cafes".

40 Pranesh Prakash, *Short Note on IT Amendment Act, 2008*, CENTRE FOR INTERNET AND SOCIETY (Feb. 2009), http://cis-india.org/internet-governance/publications/it-act/short-note-on-amendment-act-2008.

41 Pranesh Prakash, *CIS Para-wise Comments on Intermediary Due Diligence Rules, 2011*, CENTRE FOR INTERNET AND SOCIETY (Feb 25, 2011, 04:45), http://cis-india.org/internet-governance/blog/intermediary-due-diligence.

42 Prashant Iyengar, *CIS Para-wise Comments on Cyber Café Rules, 2011*, CENTRE FOR INTERNET AND SOCIETY (Feb 25, 2011, 03:30), http://cis-india.org/internet-governance/blog/cyber-cafe-rules.

43 The rules do not define the term.

44 Rishabh Dara, *Intermediary Liability in India: Chilling Effects on Free Expression on the Internet*, CENTRE FOR INTERNET AND SOCIETY (Nov. 16, 2013), http://cis-india.org/internet-governance/chilling-effects-on-free-expression-on-internet/intermediary-liability-in-india.pdf (explaining the methodology of the experiment and its results).

45 This brings to mind the way Klement Gottwald, the Czech communist leader, had Vladimír Clementis, a fellow senior member of the Communist Party of Czechoslovakia, erased from a photograph of the two of them standing next to each other, after Clementis was indicted in the Slánský show trial. In his novel The Book of Laughter and Forgetting, Milan Kundera describes this episode, and then has a character state the book's most famous line: "The struggle of man against power is the struggle of memory against forgetting." MILAN KUNDERA, THE BOOK OF LAUGHTER AND FORGETTING 4 (Aaron Asher trans., HarperPerennial 1996) (1978).

46 Dara, *supra* note 44.

47 This section includes material I've previously published on the Centre for Internet and Society's Internet Governance blog.

48 State of Madras v. V.G. Row, 1952 S.C.R. 597, 598.

49 In another chapter of this book, Andrews Rens considers the South African law (which is similar) and the principles of natural justice in some detail.

50 *See* Pranesh Prkash, *E-Books Are Easier to Ban Than Books*, OUTLOOK MAG. (Jan. 27, 2012), http://www.outlookindia.com/article/Ebooks-Are-Easier-To-Ban-Than-Books-/279712.

51 *See About Us*, CHILLING EFFECTS CLEARINGHOUSE, https://www.chillingeffects.org/about (last visited May 15, 2014).

52 *See* Pranesh Prakash & Rishabh Dara, *Counter-proposal by the Centre for Internet and Society: Draft Information Technology (Intermediary Due Diligence and Information Removal) Rules, 2012*, CENTRE FOR INTERNET AND SOCIETY, http://cis-india.org/internet-governance/counter-pro-

posal-by-cis-draft-it-intermediary-due-diligence-and-information-removal-rules-2012.pdf

53 *See* Venkateshwara Theatre v. State of Andhra Pradesh and Ors., (1993) 3 S.C.R. 616. ("Just a difference in treatment of persons similarly situate leads of discrimination, so also discrimination can arise if persons who are unequals, i.e. differently placed, are treated similarly . . . . A law providing for equal treatment of unequal objects, transactions, or persons would be condemned as discriminatory if there is absence of rational relation to the object intended to be achieved by the law.")

54 "Actual knowledge" is a requirement of Section 79(3)(b) of the IT Act, which states: "upon receiving actual knowledge, or on being notified by the appropriate Government or its agency that any information, data or communication link residing in or connected to a computer resource controlled by the intermediary is being used to commit the unlawful act, the intermediary fails to expeditiously remove or disable access to that material on that resource without vitiating the evidence in any manner."

55 Nirmaljit Singh Narula v. Indijobs at Hubpages.com, CS (OS) No.871/2012 (Delhi H.C., Mar. 30, 2012), 187234253 Indian Kanoon ¶ 15, http://indiankanoon.org/doc/187234253/.

56 The Delhi High Court's reading of the law seems to be contradictory to the 'clarification' that the Department of Electronics and Information Technology offered in March 2013 through a statement on its website: "It is clarified that the intended meaning of the said words is that the intermediary shall respond or acknowledge to the complainant within thirty six hours of receiving the complaint/grievances about any such information as mentioned in sub-rule (2) of Rule 3 and initiate appropriate action as per law. Further, the Grievance Officer of the intermediary shall redress such complaints promptly but in any case within one month from the date of receipt of complaint." *Clarification on the Information Technology (Intermediary Guidelines) Rules, 2011 under Section 79 of the Information Technology Act, 2000*, DEP'T OF ELECTRONICS & INFO. TECH., http://deity.gov.in/sites/upload_files/dit/files/Clarification%2079rules%281%29.pdf. Interestingly, in May 2011 the Department of Electronics and Information Technology had stated, "In case any issue arises concerning the interpretation of the terms used by the Intermediary, which is not agreed to by the user or affected person, the same can only be adjudicated by a Court of Law. The Government or any of its agencies have no power to intervene or even interpret." But it proceeded to do exactly that in its "Clarification" of March 2013, essentially disagreeing both the with court's interpretation as well as its own previous statement.

57 *Id*.

58 Ministry of Communications & Information Technology, *Exemption from Liability for Hosting Third Party Information: Diligence to be Observed under Intermediary Guidelines Rules*, PRESS INFO. BUREAU (May 11, 2011, 16:36), http://pib.nic.in/newsite/erelease.aspx?relid=72066.

59 Nicholas Bramble explores this idea in depth in his forthcoming paper tentatively titled, "Speech and Safety Laboratories", which he presented at the Freedom of Expression Scholars Conference 2014 held at Yale University in May 3, 2014.

60 The mainstream media also completely ignored the Cyber Cafe Rules, though those rules not only barred anonymous usage of cybercafes, but also required cybercafe operators to record the web-browsing histories of all their customers.

61 *See* Heather Timmons, *India Asks Google, Facebook to Screen User Content*, N.Y. TIMES: INDIA INK (Dec. 5, 2011, 06:33), http://india.blogs.nytimes.com/2011/12/05/india-asks-google-

facebook-others-to-screen-user-content/.

62 *See* Pranesh Prakash, *Press Coverage of Online Censorship Row*, CENTRE FOR INTERNET AND SOCIETY (Dec. 8, 2011), http://cis-india.org/internet-governance/blog/press-coverage-online-censorship

63 Judge Kumar notes in his summons order:

> *It seems that instead of regulating the undesirable and offensive content they have promoted the same for increasing the profits and promoting their business. They have closed their eyes and promoted obscene[,] derogatory[,] defamatory[,] and inflammatory material continuously on their network. It appears from a bare perusal of the documents that* prima facie *the accused in connivance with each other and other unknown persons are selling, publicly exhibiting[,] and have put into circulation obscene, lascivious content which also appeals to the prurient interests and tends to deprave and corrupt the persons who are likely to read, see or hear the same.*

Vinay Rai v. Facebook India and Ors., Summons Order, Dec. 23, 2011, *available at* http://cis-india.org/internet-governance/resources/vinay-rai-v-facebook-summons-order-2011-12-23.

64 *See, e.g.*, Danish Raza, *Sibal Not a Lone Crusader for Internet Censorship: Meet the Others*, FIRSTPOST (Dec. 26, 2011), http://www.firstpost.com/india/sibal-not-a-lone-crusader-for-internet-censorship-meet-the-others-166052.html; Amol Sharma, Is India Ignoring its own Internet Protections?, WALL ST. J.: INDIA REAL TIME (Jan. 16, 2012), http://blogs.wsj.com/indiarealtime/2012/01/16/is-india-ignoring-its-own-internet-protections/; Aparna Viswanathan, Op-ed, *The Curious Case of Vinay Rai* , HINDU (Feb. 15, 2012), http://www.thehindu.com/todays-paper/tp-opinion/the-curious-case-of-vinay-rai/article2894391.ece; and Danish Raza, *Vinay Rai vs Facebook: Govt Uses Courts to Censor the Internet*, FIRSTPOST (Jan. 13, 2012), http://www.firstpost.com/india/vinay-rai-vs-facebook-govt-uses-courts-to-censor-the-internet-181603.html.

65 There are various linkages between the violence in Assam and in Myanmar, and the resultant censorship. For a comparison of the similarities and differences in two situations, see Subir Bhaumik, *Assam Violence Reverberates Across India*, AL JAZEERA (Aug. 16, 2012), http://www.aljazeera.com/indepth/features/2012/08/201281572950685537.html. *Compare* B. Raman, Op-ed, *India: Fissures in Assam: Sons of Soil vs Bangladesh Intruders*, EURASIA REV. (July 29, 2012), http://www.eurasiareview.com/29072012-india-fissures-in-assam-sons-of-soil-vs-bangladesh-intruders-oped/ (equating the Muslims in Rakhine and in Assam as illegal immigrants from Bangladesh). There were also instances of photos from an earthquake in Tibet, and other such images being falsely circulated in Pakistan, India, and elsewhere as evidence of the mass murder of Rohingyas in Myanmar, while, as an example, gruesome photos of two rape-murder victims in El Salvador were circulated as being photos of Hindus decapitated and dismembered by Muslims in Assam. *See* Yousuf Saeed, *How to Start a Riot out of Facebook*, KAFILA (Aug. 13, 2012), http://kafila.org/2012/08/13/how-to-start-a-riot-out-of-facebook-yousuf-saeed/; *see also* Faraz Ahmed, *Social Media Is Lying to Your About Burma's Muslim 'Cleansing'*, Express Tribune: Media Watchdog (July 19, 2012), http://blogs.tribune.com.pk/story/12867/social-media-is-lying-to-you-about-burmas-muslim-cleansing/; and Pranesh Prakash, *Pranesh Prakash on Twitter: Gruesome & graphic example of hate speech & incitement to violence using lies abt Hindu women being raped & decapitated http://goo.gl/TdGnA*, Twitter (Aug 22, 2012, 16:27), https://twitter.com/pranesh_prakash/status/238417175965212672.

66 *See, e.g.*, Harichandan Arakali, *Thousands Flee Bangalore over Assam Violence*, REUTERS (Aug. 16, 2012), http://in.reuters.com/article/2012/08/16/bangalore-assam-north-east-bodo-idINDEE87F0BU20120816.

67 Even things that couldn't be blocked by ISPs, like HTML tags and Twitter user handles were requested to be blocked by the government's orders. *See* Prakash, *infra* note 68.

68 *See* Pranesh Prakash, *Analysing the Latest List of Blocked Sites (Communalism & Rioting Edition)*, CENTRE FOR INTERNET AND SOCIETY (Aug. 22, 2012), http://cis-india.org/internet-governance/blog/analysing-blocked-sites-riots-communalism.

69 *See* Pranesh Prakash, *Arbitrary Arrests for Comments on Bal Thackeray's Death*, CENTRE FOR INTERNET AND SOCIETY (Nov. 19, 2012), http://cis-india.org/internet-governance/blog/bal-thackeray-comment-arbitrary-arrest-295A-66A.

70 *See* Pranesh Prakash, *Breaking Down Section 66A of the IT Act*, CENTRE FOR INTERNET AND SOCIETY (Nov. 25, 2012), http://cis-india.org/internet-governance/blog/breaking-down-section-66-a-of-the-it-act.

CHINA

E-COMMERCE THIRD-PARTY PLATFORMS AS GATEKEEPERS OF INFORMATION FLOWS

Hong Xue

The development of e-commerce in China has been phenomenal.[1] Each year on November 11, the so-called "Singles Day", the Chinese e-retailing market witnesses a yearly online shopping carnival. Over twenty-four hours on November 11, 2013, a total of 402 million people visited Alibaba's Taobao and Tmall,[2] which are the biggest e-retailing platforms in China, and bought placed 204 million orders[3] for goods worth RMB 35.02 billion (US$ 5.75 billion),[4] an increase of RMB 15.92 billion, i.e., 83%, over the previous day.[5] This tremendous development of e-commerce has brought it into the mainstream of the Chinese economy, but nevertheless e-commerce's full market potential is yet to be discovered by the Chinese population.

While the stakeholders in the e-commerce space might seem disparate, covering everything from individual who re-sell used goods to auction sites to specialised online retailers, the "third-party platform" (TPP) — a platform where sellers and buyers come together — are the nexus of this space. These platforms are shaping the ecosystem of online commercial transactions and defining the future of the cyber-economy. Given their importance from the point of view of the public interest, and the central role they occupy in commerce and the flow of information, this paper tries to examine the TPPs' powers and responsibility in China's legal and regu-

latory environment, as well as the accountability mechanisms they are subject to.

The technical architecture of the Internet, including mechanisms the control what and how information can and cannot be transmitted across the Internet — such as Internet filtering software, encryption programs and the basic architecture of the TCP/IP protocol — have the *de facto* effect of regulating information flow over the Internet. It is arguable that all other modes of the Internet regulation either rely on, or are significantly affected by, the Internet's technical architecture. Private intermediaries occupy a central role in the techno-political landscape of Internet regulation, as they are embedded in the technical architecture of the Internet itself. The growing power of intermediaries like TPPs has turned them into tools of online regulation, illustrating the interconnected role of economic and state power in regulating online activity.

OVERVIEW

In e-commerce, a TPP isn't merely a website where sellers and buyers meet; it is a platform that provides the transactional facilities, lays the rules to be followed, and also provides other related services to the transacting parties. The function and status of a TPP may be viewed from the perspective of technology and neutrality.

Since the Internet as a whole is a platform, TPPs are like islands, big or small, on the ocean of the Internet. A TPP is, foremost, a network information system. It is a service provider enabling and facilitating the transactions, but not a contractual party, *per se*, in any particular transaction. Notwithstanding its core function of being a commercial transactional space, a platform may affiliate with, or even assimilate, many related services, like social media, instant communications, or information location tools. Its technology's design, along with the transactional rules it promulgates, may substantially affect all the parties using the platform. Importantly, those transactional rules may even affect those outside the platform.

TPPs provide a virtual trading platform, allowing sellers, including individuals and corporate entities, to publish information about goods or services and engage in trade with buyers. The sales contract is between the seller and the buyer — the TPP is not a party to the sale — and it is the

seller who is responsible for sales-related issues like the warranty and after-sale services. While TPPs provide information hosting space, allowing for sellers to advertise their goods or services, they do not exercise any editorial oversight over that information. TPPs mainly earn their profit by collecting fees from sellers' operation of virtual online stores, and providing keyword-related advertising services.

The defining characteristic of TPPs is their neutral status with respect to both sellers and buyers (collectively, "subscribers"). In some countries, a TPP is legally required to keep its TPP services separate from any other businesses it may be operating, to ensure its neutrality, with legal consequences ensuing if it compromises its neutrality. Where a TPP's own sales business, for instance, is not separable from its third-party platform services, the TPP shall be responsible for compensating those consumers suffering from the purchase of any unqualified and/or counterfeit goods sold on the platform, irrespective of whether the goods were sold by the TPP provider directly.[6]

As a neutral third party, the TPP provider plays a bigger role than any of the subscribers to the platform. Its unique technological capacity and neutrality status grant it *de facto* governance power in its own system. A TPP's power is particularly demonstrated through the transactional rules it sets out as the standard terms to be included in all the relevant contracts that are binding on subscribers, and also impacts third parties, such as intellectual property (IP) owners whose rights or interests might be affected.

TPPs are thus evolving into a sophisticated, large-scale, technologically-capable and commercially-powerful transactional ecosystems on the Internet. Therefore, a TPP's powers ought to be balanced by appropriate duties, along with mechanisms for accountability, which would secure not only the legitimate interests of all the subscribers to the platform, but also the interests of the public at large.

POWERS OF TPP PROVIDERS

The main power that a TPP has is that of establishing, and enforcing, policies and rules concerning the use of the platform. Thus, the TPP provider, although not a direct party to any of the transactions between sellers and buyers, is able to regulate all the subscribers via its policies and

rules, and thus control the whole ecosystem in a manner far greater than the kind of control exerted by, say, a shopping mall over a traditional brick-and-mortar establishment operating in it.

All TPP-made policies and rules applicable on a platform taken together constitute the transactional rules, which are the open norms set out and enforced by that TPP provider, binding on all subscribers, and impacting other right-holders as well as the public interest. Though the transactional rules are applicable to all subscribers, they are unilaterally established by each TPP provider.

Based on an empirical study of six leading TPPs in China, i.e., Taobao, Tmall, Jingdong Online Mall, Tencent Paipai, Dangdang and Amazon.cn, the transactional rules — in the forms of terms of service (ToS), terms of use (ToU), public announcements, end-user agreements, etc. — may be divided into the following categories:

- Transactional security measures, defining subscribers' eligibility and transactional validity and enforceability;
- Rules on liabilities and risks, defining the TPP provider's liability, limit, exemption and indemnity to the other parties;
- IP policies and measures, protecting IP rights of all parties involved;
- Credit assessment mechanism, assessing the credit of both sellers and buyers;
- Consumer protection and data protection measures;
- Content regulation measures;
- Penalty and dispute resolution;
- Applicable subjects, coverage and term;
- Rules on amendment of the rules;
- Other rules.[7]

Although similar to standard form contracts in terms of their unilateral and non-negotiable nature, a TPP's transactional rules' complexity, universality and global outreach set them apart. A subscription to a TPP is much more complicated than the simple conclusion of a contract with another party.

After years of development, the transactional rules of the TPPs, particularly those market-dominant platforms, like Alibaba, have become sophisticated normative systems, with various forms, scopes of coverage,

subjects, targets, and with frequent updates. Some of the rules are expressed in the form of standard-term contracts between the subscribers and the TPP provider.[8] But most rules, including the punitive ones, are applied to all subscribers by default, irrespective of whether a subscriber has explicitly expressed consent.[9] Thus, by using a service, the subscriber actually enters into a space governed by the TPP provider through a body of transactional rules that are frequently changed unilaterally.[10]

In addition to their universality, unilateralism and global nature, TPPs' transactional rules have the characteristic of externality that is distinct from traditional standard form contracts. Apart from the obvious application to the subscribers' contracts with the TPP provider, the transactional rules apply to the contracts between a subscribed buyer, a subscribed seller and the other parties that are not subscribed to the platform services at all, such as the IP owners whose trademarks or copyrighted works are involved on the platform. Most mature TPPs have implemented measures to protect IP owned by both subscribers and non-subscribers.[11] For example, many TPPs' transactional rules enable a copyright or trademark holder to complain against piracy or counterfeiting occurring on the platform, even though the right-holder has no contractual relationship with the TPP provider. The transactional rules, therefore, impact non-subscribers' rights and interests too.

Thus, it's amply clear that a TPP's body of transactional rules constitutes the "by-laws" of that platform. Even though the TPP is a third party to a transaction between a seller and a buyer, the TPP's rules are always applicable and binding on the transacting parties. If a dispute occurs in the transaction, the TPP may be empowered to adjudicate between the parties, and resolve the dispute. Since a TPP is like a digital territory or frontier on the Internet, superseding physical state boundaries, its transnational rules actually govern that virtual space and define the legal relationships of the stakeholders involved.

RESPONSIBILITIES OF TPPS

The TPP's power to regulate, define and affect the transactions and the parties on or off the platform is both substantive and significant. The Internet, however, is not a lawless space. It is clear that conduct that is unlawful offline is presumptively unlawful online, and subject to similar laws

and regulations. Areas like gambling, child pornography, and fraud are regulated in very similar ways online as well as offline. The TPPs and the transactions conducted on the Internet, naturally, are not immune from legal regulation.[12] There have been many cases where the transactional rules of the TPPs have been struck down in either judicial or administrative proceedings. This legal evolution shows that the TPPs must pay heed to the responsibilities to the various stakeholders, particularly to the state authorities.

TPP providers, despite their global operation, are subject to differing legal obligations and requirements in different countries. The TPP providers' compliance with these obligations and requirements may or may not be connected with their transactional rules. For example, under the recently-disclosed "PRISM" programme, the United States' National Security Agency has the authority to unilaterally search and access materials stored on servers operated by nine leading US Internet businesses to target foreigners, with the ability to extract audio, video, photographs, e-mails, documents and connection logs. The participating technology companies, reportedly including Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Skype, YouTube, and Apple, cannot even disclose this highly classified program and their involvement.

In China, all TPPs must comply with the legal requirements specified in the Measures on the Administration of Internet Information Services (IIS Measures),[13] which applies to any service activity of providing information through the Internet to online subscribers.[14] Under Article 15 of the IIS Measures,[15] online information service providers may not produce, reproduce, disseminate or broadcast illegal information with content that:

- opposes the fundamental principles determined in the Constitution;
- compromises state security, divulges state secrets, subverts state power or damages national unity;
- harms the dignity or interests of the state;
- incites ethnic hatred or racial discrimination or damages inter-ethnic unity;
- sabotages state religious policy, or propagates heretical teachings or feudal superstitions;
- disseminates rumours, disturbs social order, or disrupts social stability;

- propagates obscenity, pornography, gambling, violence, murder, or fear, or incites the commission of crimes;
- insults or slanders a third party or infringes upon the lawful rights and interests of a third party; or,
- includes other content prohibited by laws or administrative regulations.

Under the IIS Measures, the online information service providers that engage in news, publishing or electronic bulletin board services, etc., shall keep a record of the information they provide, the time-stamps and the Internet addresses or domain names of that information;[16] the Internet access service providers shall keep a record of such information as the times online subscribers are online, the subscribers' account numbers and their URLs or domain names, and the subscribers' telephone numbers.[17] Both the online information service providers and Internet access service providers shall keep copies of such records for 60 days and shall provide them to the relevant state authorities when the latter make inquiries in accordance with the law.[18] If an online information service provider discovers information transmitted through its website that is clearly illegal, it shall immediately stop the transmission thereof, save the relevant records and make a report thereon to the relevant authority.[19]

With the growth of e-commerce, the Chinese governmental departments are strengthening the regulation of TPPs. For instance, in May 2010, the State Administration for Industry and Commerce released new interim measures strengthening consumer protection online, and laying out obligations of online sellers as well as TPPs.[20] In 2014, after going through a public comments process,[21] a revised version of the measures were passed.[22] In April 2011, the Ministry of Commerce put out a set of service norms, effectively a code of conduct, for TPPs and their subscribers.[23] In July 2011, the State Administration for Industry and Commerce, the Ministry of Public Security, the Ministry of Commerce and six other ministries and departments jointly published a new notice relating to IP infringement on TPPs.[24]

Most importantly, in September 2013, the Ministry of Commerce published a draft of the proposed Administrative Measures on Transactional Rules of Third-Party Platforms for Internet Retail (draft Measure on Transactional Rules) for public consultation.[25] Under the draft measures, a

TPP's transactional rules are subject to direct legal regulation and review. The TPP must ensure the safety, accuracy and integrity of the trade data, and the servers that store the trade data must be located within Chinese legal jurisdiction. For the purpose of consumer protection, the draft measures also requires that a TPP distinguish between advisements and normal search results so that the subscribers would not be confused between them.

TPPs have been forced to assume more responsibilities with respect to content regulation as well. In August 2013, all Internet businesses were required to publicly commit to the "seven bottom lines": of law and regulations, of a socialist system, of state interest, of legitimate citizens' rights, of social public order, of morality, and of information truthfulness. On September 6, 2013, China's Supreme People's Court and Supreme People's Procuratorate jointly issued an opinion on 'Handling the Criminal Cases of Defamation via Utilization of Information Network',[26] under which anyone whose defamatory post on the Internet was viewed more than 5,000 times or "re-tweeted"/shared more than 500 times is subject to severe criminal punishment.[27] The new requirements on content regulation have pushed the TPP providers to strengthen their information filtering measures.

The TPP's increasing legal obligations for intellectual property protection, on the other hand, impact the flow of information on their platforms. A TPP provider should, of course, respond to the orders of the courts or the competent authorities regarding the protection of intellectual property rights, such as removing immediately any infringing remarks or information. In addition, a TPP is obliged to implement its own right-protection measures to prevent or terminate in a timely manner the infringing activities on the platform. Failure to take necessary measures may cause the TPP provider liable to the intellectual property owners.

In a case against Apple, the Encyclopedia of China Publishing House asserted that the Cupertino-based company was liable for the sale of unauthorized digital copies of its encyclopedia through Apple's App Store. Apple argued that as the store owner — and not an app developer — it was not responsible for every individual application hosted in the App Store. The court, however, ruled that Apple was responsible as it both approved and profited from the app's sale. Apple was ordered to pay RMB Yuan

520,000 (US$82,600) to compensate the Publishing House.[28] In April 2013, Apple consecutively lost three similar cases for copyright-infringing apps sold in the App Store.[29] These cases show that Apple, as a TPP provider, is obligated to monitor the App Store to prevent copyright infringement.

In addition to safeguarding their stores from being used for copyright infringement, the TPPs are also required to share the burden of proactively monitoring goods and services that may involve counterfeiting or trademark infringement. Under Article 36 of China's Tort Law,[30] the network service providers shall assume tort liability if it infringes upon civil rights or interests of others. If a user commits a tortious act through the network services, the victim shall be entitled to inform the service provider to take necessary measures, including, *inter alia*, deletion, blocking and disconnection.[31] If the service provider fails to take necessary measures in a timely manner upon notice, it shall be jointly and severally liable to the said victim for the damage caused by inaction.[32] Article 36 also provides that if a service provider is aware that one of its users is infringing on the civil rights and interests of others through its services and fails to take necessary measures, it shall be jointly and severally liable to the said victim for any additional harm caused by its inaction.

China's best-known and largest TPP, Taobao, has been sued for trademark infringement in more than 20 cases.[33] These cases were separately brought by companies like Puma and E-Land. In most cases, the Chinese courts held that Taobao was a mere online service provider that sufficiently complied with the notice-and-takedown requirements. For example, in a trademark infringement case decided in 2010, a court of first instance in Shanghai held that Taobao had not committed contributory infringement. In the court's reasoning, although the plaintiff had complained to Taobao several times about a particular seller's offering for sale goods falsely bearing the trademark "E-LAND" to which the plaintiff had an exclusive licence, Taobao could not verify authenticity of the plaintiff's evidence. Further, even if the authenticity could be verified, the evidence was unable to show that the complaints against the pertinent seller related to the registered trademark or the goods at issue. The court noted that upon receipt of the complaints and at the request of the plaintiff, Taobao had temporarily removed access to the information of the goods at issue and provided contact details of the seller, and fully removed access to the complained

goods after the plaintiff filed the lawsuit. Furthermore, the court held, Taobao had taken a series of measures, including real name verification and drafting of intellectual property protection measures. Therefore, the court concluded, by conducting a takedown upon notice, Taobao fulfilled its reasonable duty of care as a service provider.[34]

Taobao suffered a major setback in April 2011 when the Shanghai First Intermediate People's Court finally ruled that Taobao was jointly liable for trademark infringement for failing to effectively respond to the trademark owner's repeated takedown requests and must compensate the trademark owner RMB Yuan 10,000 (US$1,800) for damages and costs.[35] In a case involving the same complainant (Yinian, the exclusive licensee of E-Land International), a different court of first instance in Shanghai held that the removal of information by a service provider upon notice is a necessary condition, but not a sufficient condition, for exemption from compensation liability.[36] The court held that that if Taobao's users continue to infringe, it should take further measures to stop the continuing infringement. Further, it was held that Taobao should have penalized the infringing user in strict accordance with its transactional rules, noting that while this would not fully eliminate infringing activities completely, it would reduce infringing activities.[37] It also held that Taobao should be held to be aware of a seller's sale of counterfeit goods on the online trading platform given that it had received seven complaints from the plaintiff about the seller's sale or offer for sale of goods that infringed the plaintiff's exclusive right to use the "TEENIE WEENIE" trademark. The court held that Taobao, did not do anything although it was able to and in a position to take action against specific infringers, and as a result, the seller was still able to offer infringing goods for sale without any restrictions. Taobao, therefore, was held to have committed contributory infringement with subjective fault, and thus was held to be jointly liable along with the trademark infringer.[38]

Upon Taobao's appeal, the Shanghai First Intermediate People's Court upheld the ruling and found that Taobao had knowledge of the trademark infringement committed by others through its services, but Taobao only passively deleted infringing links upon notice being provided by the trademark owner and failed to take necessary measures to prevent the occurrence of the infringing acts.[39] The court held that Taobao merely removed the pages linked to the alleged infringing goods, but failed to take any

punitive actions against the seller as specified in its transactional rules, e.g., by freezing the seller's account, degrading the seller's reputation, or preventing the seller from creating new infringing listings.[40] This, the court held, showed that Taobao helped others commit infringement, and that it should be held jointly liable for the trademark infringement, and face joint compensation liability.

Under the threat of legal liability, TPP providers have been seeking the cooperation with brand owners and other intellectual property owners to exercise more effective administration over the unlawful acts on their platforms. On the other hand, the TPPs, irrespective of their power and capacity, should not be utilized to go beyond the legal limits and boundaries of intellectual property rights. Intellectual property protection should maintain a proper balance with the freedom of expression and free flow of information.[41]

In March 2011, the globally well-known paint producer Nippon Paint Co. Ltd. (Nippon) discovered that Zhanjin Co. had set up a shop on Taobao and had been using Nippon trademarks and trade dress in advertisements concerning Nippon products with no approval or licence from it. With no reply from Taobao after filing a complaint, Nippon sued Zhanjin and Taobao in court, and yet the complaint was rejected by the first instance court. Dissatisfied with this result, Nippon appealed to the Shanghai First Intermediate People's Court.

The court ruled that since the Zhanjin's use of Nippon's trademark was for product information display only, and it could not possibly lead to confusion among the public. In addition, the court ruled that no commercial interests of the plaintiff was being damaged. Based on these findings, the alleged trademark infringement claim could not be established, and therefore the original decision was upheld. Taobao, as the TPP provider, was not liable where no direct infringement of the complainant's trademark occurred.[42] The case shows that online retailers may make the non-infringing descriptive use of the trademarks, provided that the products sold in one's shop are genuine articles and not counterfeit.

ACCOUNTABILITY OF TPPS

TPPs are currently occupying a dominant position in Chinese e-com-

merce, defining the transaction process and service standards and playing a significant role in the development of the whole ecosystem. Given their legal obligations and social responsibilities, the TPPs' self-regulatory and internal accountability mechanisms should develop in proportion to their dominance.

At the end of 2011, Taobao encountered large-scale protests by sellers against its unilateral change of the subscription terms regarding the deposits and fees they needed to pay. The bitter dispute was directly sparked by a new rule issued by Taobao that resulted in a sharp increase in the annual membership fees and cash deposits for all subscribed sellers. The hikes in the annual membership fees and cash deposits undoubtedly placed some small business owners in a dilemma: facing up to unaffordable fees and deposits or giving up their early investments in the virtual stores that had been built on the platform. Those small business owners felt that they were cornered by Taobao, and so protested. Thousands of angry small business owners and netizens formed a so-called "Anti-Taobao Union" and caused certain large sellers of brand-name products to suffer heavy losses by placing orders and cancelling them after leaving disparaging remarks. China's Ministry of Commerce had to intervene to calm the situation down in October 2011. The Ministry commanded that Taobao actively respond to the legitimate needs of small business owners, and their protests against the fee increases within legal parameters. The "union" stopped protesting after the Ministry stepped in. Taobao promised to be more cautious and responsible when making any substantial change to the transactional rules in the future but insisted on raising the annual fees charged to the sellers.

In the 2011 incident, Taobao attempted to elevate the sellers' access threshold so as to prevent a flood of counterfeit goods and endless consumer complaints. Although Taobao has the complete discretion to change and/or update the rules applicable to the platform, the incident drew the public's attention to TPP providers' social responsibility towards small and medium enterprises that rely on their ecosystem to survive and grow. And though this social responsibility might appear to be no more than a moral duty, it can also incur governmental intervention and legal supervision.

For the government too, the 2011 Taobao incident was a wake-up call to

the issue of TPPs' accountability. The Ministry of Commerce, after making *suo motu* interventions in the dispute, took action to supervise Taobao's accountability mechanism. In the draft Measures on Transactional Rules, TPP providers are required to publish their proposed changes to the transactional rules for public comments 30 days before its adoption, and to provide transitional measures for the subscribers, if necessary. Although the mandatory public disclosure requirement cannot fully address the TPPs' accountability issue, it can at least lead to greater oversight of TPP providers' procedures.[43]

CONCLUSION

The development of TPPs in the Chinese economy has seen remarkable expansion in less than two decades. Although not a party to any specific transaction between a seller and a buyer, a TPP actually *governs* all the subscribers and non-subscribers through a matrix of transactional rules in different categories and on different subjects. As the nexus of Chinese e-commerce, TPPs have acquired considerable power to regulate, define and affect commercial transactions and various stakeholders. It is arguable whether the TPPs are becoming *global regulators* via their global operation and globally-applicable transactional rules.

This chapter attempts to analyse the dynamics of TPPs and the existing legal framework. Content regulation occupies a large presence in the Chinese regulatory environment. TPP providers, like Alibaba, are developing and adopting comprehensive policies to monitor the information contents flowing through transactional processes. The enforcement of compliance with TPP providers' transactional rules provides an interesting addition to law enforcement measures relating to content regulation, and have significant impact on the free flow of information. The legality, validity and enforceability of these by-laws deserve careful legal examination and assessment.

1 *See* Frank Tong, *Bain Predicts China Will Overtake the U.S. in E-Commerce This Year*, INTERNET RETAILER (Sept. 3, 2013), http://www.internetretailer.com/2013/09/03/bain-says-china-will-overtake-us-e-commerce-year (noting that between 2009 and 2013, e-commerce in China grew at a compounded annual rate of 71 per cent).

2 He Wei, *11+11 Is a Winning Formula*, CHINA DAILY (Nov. 15, 2013), http://epaper.chinadailyasia.com/asia-weekly/article-1416.html.

3 Alex Pitti, *Forget Cyber Monday, Singles Day Is The Focus For Alibaba*, SEEKING ALPHA (Sep 19, 2014), http://seekingalpha.com/article/2506425-forget-cyber-monday-singles-day-is-the-focus-for-alibaba.

4 That figure merely counts the amount that was spent on Taobao and Tmall using Alipay, Alibaba's in-house payment gateway. Wei, *supra* note 2. The overall spending, counting other platforms — like Suning, 360Buy, Dangdang and Amazon's Chinese website — and other methods of payment would further increase the finally tally.

5 For comparison, the equivalent in the United States, Cyber Monday, saw an industry-wide estimated sales figure of US$ 1.74 billion in 2013. Press Release, comScore, Cyber Monday Jumps 18 Percent to $1.735 Billion in Desktop Sales to Rank as Heaviest U.S. Online Spending Day in History (Dec. 3, 2013), https://www.comscore.com/Insights/Press-Releases/2013/12/Cyber-Monday-Jumps-18-Percent-to-1735-Billion-in-Desktop-Sales-to-Rank-as-Heaviest-US-Online-Spending-Day-in-History.

6 In a recent case, Dangdang, a leading TPP provider in China, was ordered by the court to compensate a consumer ten times the purchase price of the counterfeit goods that had been bought, since the manufacturer had a fake name and address. The court ruled that the consumer was only able to identify the operator of the platform but could not determine the appropriate companies behind the supply chain. The court ruled that since Dangdang had issued the invoice to the consumer, it should be responsible as the seller. Wang v. Beijing Dangdang Information Technology Co., Ltd., Beijing Chaoyang District People's Court (March 2013).

7 The transactional rules cover a wide range of topics, such as user rights and responsibilities; proper or expected usage; accountability for online actions, behavior, and conduct; privacy policies; payment details such as membership or subscription fees, etc.; limitation of the TPP's legal liability for damages incurred by users; and user notification upon modification of terms, if offered.

8 For example, there are the terms of service agreements on collection, storage and process of a user's personal data. A legitimate terms of service agreement is legally binding, but may be subject to change.

9 Since transactional rules are regularly updated as per the market situation and management needs, many TPP merely set out the amendment/updating procedures, rather than let all the subscribers confirm their consent to any new rules or policy. A subscriber, who continues to use the platform services, is presumed to consent to the changed or updated rules.

10 Like an experimental application programming interface (API), these are often permissive rules at first, with tighter restrictions over time.

11 Many TPPs reserve or claim the intellectual property rights in user-generated content (UGC) through their transactional rules.

12 Although most countries only regulate the conducts of the TPPs, some countries have set out the market access threshold to the TPPs. Only those operators that pass through the financial, technical and manageable capacity assessment can acquire the administrative license to become the TPP providers. For example, Chinese Ministry of Commerce is drafting the Ministerial Administrative Measures to define the market entry criteria for the TPP providers.

13 Measures on the Administration of Internet Information Services (promulgated by the State Council, Sept. 25, 2000, effective Sept. 25, 2000), *translation available at* http://www.wipo.int/edocs/lexdocs/laws/en/cn/cn111en.pdf.

14 *Id.*, art 2.

15 *Id.*, art. 15.

16 *Id.*, art. 14.

17 *Id.*

18 *Id.*

19 *Id.*, art. 16.

20 *See generally* Interim Measures for the Administration of Online Commodities Trading and Relevant Services (promulgated by the State Admin. for Indus. & Com., May 31, 2010, effective July 1, 2010), *translation available at* http://uip-law-firm.com/en/newsView.asp?id=246.

21 *See China Solicits Comments on the New Administrative Measures for Online Commodity Trading*, CHINA BRIEFING (Sept. 20, 2013), http://www.china-briefing.com/news/2013/09/20/china-solicits-comments-on-the-new-administrative-measures-for-online-commodity-trading.html.

22 Measures for the Administration of Online Transactions (promulgated by the State Admin. for Indus. & Com., Jan. 26, 2014, effective Mar. 15, 2014). For further analysis of the rules, see David L. Woronov, *China Adopts New Administrative Measure To Protect Internet Privacy And Personal Information*, Metropolitan Corporate Counsel (Apr. 18, 2014), http://www.metrocorpcounsel.com/articles/28465/china-adopts-new-administrative-measure-protect-internet-privacy-and-personal-informa.

23 Service Norms for Third-party E-commerce Transaction Platforms (promulgated by the Ministry of Com., Apr. 12, 2011), *translation available at* http://www.lawinfochina.com/display.aspx?lib=law&id=8810.

24 *See* Luo Yushu, *Determination of Joint Liability for Trademark Infringement in Online Trading*, CHINA DAILY: CHINA INTELLECTUAL PROPERTY (Mar. 12, 2012), http://ipr.chinadaily.com.cn/2012-03/12/content_14815056.htm (mentioning the Notice on the Implementation Plan for the Special Campaign to Crack Down on the Infringement of Intellectual Property Right and the Manufacture and Sales of Counterfeit and Substandard Commodities in the Online Shopping Area).

25 Shāngwù bù guānyú "wǎ ngluò língshòu dì sānfāng píngtái jiāoyì guīzé guǎ nlǐ bànfǎ (zhēngqiú yìjiàn gǎ o)" gōngkāi zhēngqiú yìjiàn [Ministry of Commerce on "Administrative Measures on Transactional Rules of Third-Party Platforms for Internet Retail (Draft)" for Public Comment], Sept. 26, 2013, http://tfs.mofcom.gov.cn/article/as/201309/20130900322643.shtml. *See China Release Draft Plan to Develop its Online Retail Industry*, CHINA BRIEFING (Oct. 4, 2013), http://www.china-briefing.com/news/2013/10/04/china-to-vigorously-develop-online-retail-industry.html; *see also* Roy Zhou et al., *China Seeks to Update its Legisla-*

tion to Address Burgeoning E-Commerce Market, HOGAN LOVELLS (Dec. 2013), http://www.hoganlovells.com/files/Uploads/Documents/13.12.03_China_seeks_to_update_its_ecommerce_laws_HKGLIB01_1071582_Final_4.pdf (providing in-depth analysis of the new regulations and their significance).

26 Interpretation of the Supreme People's Court and the Supreme People's Procuratorate on Several Issues Concerning the Application of Law in the Handling of Criminal Cases on the Use of Information Networks to Commit Defamation and Other Similar Criminal Offences (promulgated by Sup. People's Ct. & Sup. People's Proc., Sep. 6, 2013, effective Sep. 10, 2013). While there is no system of *stare decisis* in China, the Supreme People's Court has the authority to issue judicial interpretations as guidelines to trials, which are nationally enforceable. *Legal Research Guide: China*, UNITED STATES LIBRARY OF CONGRESS, http://www.loc.gov/law/help/legal-research-guide/china.php.

27 The Summer of 2013 ended with many sensational social dramas, all of which centered around Sina Weibo, the Chinese equivalent of Twitter. The live streaming on Sina Weibo of the trial of the corruption case of Bo Xilai, a former member of the Politbureau and former Chief Party Secretary of CCP in Chongqing, shows the new level of transparency and openness in Chinese political life and judicial system. On the other hand, the arrest of a number of influential social commentators and independent intellectuals (so-called "Big V") alleged of spreading untruthful information or rumours via Sina Weibo shows that all the communications and expressions are actually closely monitored on the seemingly open and free Internet. Big V does not mean "V for Vendetta". Originally, it refers to those "verified" Weibo account holders marked by the letter "V". It gradually started to refer to those people who are vocal on the social matters, particularly on governmental corruption and social injustice.

28 Encyclopedia of China Publishing House v. Apple Inc. (Beijing No. 2 Interm. People's Ct., Sept. 27, 2012). *See* Josh Ong, *Chinese Encyclopedia Wins $86,000 in Lawsuit Against Apple over App Store Piracy*, Next Web (Sept. 28, 2012), http://thenextweb.com/asia/2012/09/28/chinese-encyclopedia-wins-86000-lawsuit-apple-app-store-piracy.

29 In these cases, Beijing Motie Digital Alliance Information Technology Ltd, Mai Jia, and Yu Zhuo claimed that Apple allowed pirated versions of their works to be sold through the App Store. Apple was ordered to pay the three copyright holders more than RMB Yuan 700,000 (roughly US$ 12,000), although the complainant had demanded the compensation for US$ 3.65 million. In December 2012, 8 Chinese authors won another copyright infringement lawsuit against Apple. These authors are some of China's most popular, gracing best-seller lists throughout the country. Their books were offered for download on Apple's App Store without authorization from the writers. The court ordered Apple to pay a total of RMB Yuan 412,000 (US$ 66,000) for compensation.

30 Tort Law (promulgated by Standing Comm. Nat'l People's Cong., Dec. 26, 2009, effective Jul. 1, 2010), art. 36, *translation available at* http://www.wipo.int/wipolex/en/text.jsp?file_id=182630.

31 *Id*.

32 *Id*.

33 In a trademark infringement case in 2005, Puma AG Rudolf Dassler Sport sued Taobao and a store owner Chen Yangrong. Puma named Taobao as the first defendant and blamed Taobao for publishing and selling goods that infringed upon its exclusive right to use the PUMA trademark, on the basis that Taobao's relationship with the Chen's online store was similar to

that of a shopping centre with a store, and that an Internet service provider had the same duty as the shopping centre to check infringement. The court found that a shopping centre, in its sales of goods, collects payment and issues receipts in its own name, and the sales can be deemed as an act of the shopping centre, while Taobao's users would not consider sales of online stores as an act of the platform, and that sales of online stores would not be legally considered as an act of the platform. The court held that the TPPs are technical service providers who merely publish their customers' information through electronic bulletin services. Consequently, the platforms are not, themselves, sellers but instead services providers to those who actually sell items on their sites. Being strictly liable for the legitimacy of all trading on their sites is beyond the scope of the TPP's capacity.

34 Yinian (Shanghai) Garments Trading Co., Ltd. v. Xu & Zhejiang Taobao Network Co., Ltd. (Shanghai Huangpu District People's Ct., 2010).

35 Yinian (Shanghai) Garments Trading Co., Ltd. v. Zhejiang Taobao Network Co., Ltd. & Guofa Du (Shanghai No.1 Interm. People's Ct., Apr. 25, 2011). For a more detailed overview of the case, see Zhu Zhi Gang & Paul Ranjard, *Analysis on the Taobao Case*, WAN HUI DA (July 29, 2011), http://www.wanhuida.com/Portals/1/YRNewsAttachment/719/wanhuida_analysis_on_taobao_case.pdf; *see also* Chen Jianmin, *Case Comment: Yinian (Shanghai) Garments Trading Co., Ltd. v. Zhejiang Taobao Network Co., Ltd. and Du Guofa*, 4 TSINGHUA CHINA L. REV. 283 (2012) (welcoming the court's holding of Taobao liable, while regretting that it didn't impose a higher penalty).

36 Yinian (Shanghai) Fashion Trade Co. Ltd. v. Zhejiang Taobao Network Co., Ltd. & Du Guofa (Shanghai Pudong New District People's Ct., Jan. 19, 2011).

37 *Id.*

38 *Id.*

39 Yinian v. Zhejiang Taobao & Guofa Du (Shanghai No.1 Interm. People's Ct., Apr. 25, 2011).

40 *Id.*

41 *See generally* Hong Xue, *Between the Hammer and the Block: China's Intellectual Property Rights in the Network Age*, 2 U. OTTAWA L. & TECH. J. 291, *available at* http://www.uoltj.ca/articles/vol2.2/2005.2.2.uoltj.Xue.291-314.pdf (arguing, "[s]uccessful IPR policies should be proportionate to China's economic development stage, effectively preventing any abuse of IPRs, and must be interoperable with the international economic and trade system").

42 Nippon Paint Co. Ltd. v. Zhanjin Company & Taobao (Shanghai Xuhui District People's Ct., Oct. 2011, *aff'd* Shanghai No. 1 Interm. People's Ct., May 24, 2012).

43 The draft Administrative Measures on Transactional Rules of Third-Party Platforms for Internet Retail are currently being reviewed and modified by the Ministry of Commerce. It is unknown whether the draft will be adopted.

MYANMAR

BANS, BLAMING & BUDDHIST MONKS

Censorship Concerns around Myanmar's Ethno-Religious Violence and Democratic Transition

Erin Biel

A stoic U Wirathu, the 45 year-old Buddhist monk and outspoken leader of the "969" Buddhist nationalist movement in Myanmar[1], stares out from the July 1, 2013, cover of *Time* magazine. The words "The Face of Buddhist Terror" stand out from the page in white letters against the ochre-coloured robe draped around his body. The article, featured on the cover of every edition of *Time* except in the United States, explores the rise of combative nationalist Buddhism in Myanmar and throughout Asia, and focuses on U Wirathu's 969 movement, which began in 2000 and encourages the country's Buddhist majority to boycott Muslim businesses and social spaces. Written by *Time*'s East Asia Correspondent and China Bureau Chief, Hannah Beech, the piece begins by introducing U Wirathu as a self-proclaimed "Buddhist Bin Laden", which U Wirathu later claimed was a misinterpretation, having explained to the author in an interview that this was one of the many epithets he had been called by his detractors.[2] Nevertheless, the movement has been gaining in prominence ever since religious violence between Myanmar Buddhists and Muslims started in the middle of 2012, resulting in more than 250 deaths and another 140,000 fleeing their homes over the course of the next year. Most of the victims have been Muslims, who make up just four per cent of this Buddhist-majority country.

The ongoing violence, and the government's inability to stop it, have

marred the country's image as it ostensibly undergoes a democratic transition following nearly five decades of military rule. In addition, the government's attempts at preventing both domestic and international media from publishing incendiary material that could potentially stoke tensions have been seen as both an encroachment on freedom of expression and an ineffective panacea for the underlying ethnic and religious friction in the country.

While the *Time* article was behind a paywall online, both the original English version and Myanmar-language translations had already started circulating by email and social media in advance of *Time*'s July 1st print publication. By June 22, the Facebook page "We Boycott *Time* magazine for their choice of Wirathu as 'Buddhist terror'" had already attracted more than 10,000 "likes" and become a forum for criticizing both *Time* and the author of the article. As of July 15, 2013, it had over 35,000 "likes" — no small feat for a country in which only one per cent of its 60 million people is thought to have Internet access.[3] Other online petitions expressing outrage over the piece had garnered tens of thousands of signatures.[4] Meanwhile, Myanmar's President Thein Sein, viewed by many in the international community as a reformist leader,[5] posted a statement on his official website on June 23, 2013, criticizing *Time* for writing the piece, and defended Myanmar's monkhood and its long Buddhist tradition.[6] The distributor of *Time* magazine in Myanmar, Inwa Publications, decided that it would not publish the July 1 issue, which triggered concern among human rights groups. Being *Time* magazine's sole distributor in Myanmar, the privately-owned company was effectively violating media freedom and the public's right to information.[7]

On June 25, the Myanmar government officially announced that it had banned the controversial cover story in order to prevent further conflict. The Deputy Minister of Information Ye Htut posted news of the ban on his Facebook page: "The article entitled 'The Face of Buddhist Terror' in *Time* magazine 1 July issue is prohibited from being produced, sold or and distributed in original copy or photocopy in order to prevent further racial and religious conflicts." An explanation of the ban was also provided in the following day's state-run newspapers and on state-run television.[8] The President then made a monthly address on the state-run radio, in which he asked the media to report on Myanmar in a manner that provided solu-

tions to the country's problems, rather than exacerbated them:

> *According to a traditional Myanmar saying, people shouldn't say something if it is not good for others, even if it is right . . . . When people are making use of the freedom of expression, it should be done in a responsible way in light of Myanmar's society and Myanmar's current political situation. It should also be constructive.*[9]

The ban — and the rationale behind it — were largely supported by Myanmar political figures, religious figures, and journalists alike. U Than Htut Aung, the Chief Executive Officer of Eleven Media Group, one of the most popular independent media outlets in Myanmar, wrote in the *Daily Eleven* that he did not agree with many things U Wirathu had said, but "in my opinion as a journalist, the *Time* presentation of Buddhism is not fair. It is an insult to our country and Buddhism and I object to it. What is more, *Time* has disturbed our transition to democracy and provoked more conflict."[10]

After a few days of smaller-scale protests, hundreds of monks, journalists, and other protesters amassed in downtown Yangon — the largest city in Myanmar and former capital — near the iconic Sule Pagoda, carrying signs lauding President Thein Sein for his criticisms of the article and calling on *Time* magazine to stop smearing Buddhism and inciting religious conflict. The government had given special permission for the protest to occur.

This protest marked a significant turnaround from August 2012, when journalists in the city sought to demonstrate against the government for suspending two independent publications, the *Voice* and the *Envoy*, after they ran stories about a purported Cabinet restructuring without the prior approval of the now-defunct Press Scrutiny and Registration Division (PSRD), which used to oversee pre-publication censorship. Outraged, the Committee for Press Freedom (CPF), a grass-roots organization of local media figures, decided to stage a series of protests, the main one set to convene in front of Yangon's City Hall on August 21, 2012.[11] However, the police denied the group permission to protest, and the dissolution of pre-publication censorship was interestingly announced the day before the scheduled demonstration.[12]

Despite the dissolution of pre-publication censorship, other forms of censorship have taken hold. Self-censorship continues to reign, as well as other forms of government-induced censorship, as in the case of the *Time* piece. What is perhaps even more alarming is the fact that journalists and readers, unlike a year ago when the suspension of the *Voice* and the *Envoy* sparked outrage, are at times acquiescing to and even vocally advocating for the reinstatement of censorship on some types of publications as a result of the religious and ethnic violence in the country.

U Thein Sein's professed approach of preventing the publication of something that is "not good for others, even if it is right" precludes any bona fide realization of free speech and of unfettered access to information, and, moreover, fails to address the country's underlying ethnic and religious tensions. The President's June 2013 remarks on state television came on the heels of a June 28 workshop at the U.S. Embassy in Myanmar on preventing hate speech, during which the U.S. Ambassador to Myanmar, Derek Mitchell, discussed how to balance an individual's right to free speech with the rights of a society to be free from violence and conflict. In an opening address, Ambassador Mitchell averred that citizens in a democracy must not avoid controversy and that censorship "is rarely the answer".[13] Rather, he continued, "what is needed instead is an open national dialogue where all of the diverse voices of Myanmar participate, where speech is free, respectful, peaceful, and different viewpoints compete in a marketplace of ideas, without violence or intimidation."[14]

In response, Myanmar's Deputy Minister of Information Ye Htut, speaking at the conference, suggested that "media literacy" needs to be developed to prevent such hate speech on social media from being the main source of people's information. He cited the spate of religious violence in Lashio, the largest city in Shan state, in May 2013 — in which a mosque, a Muslim orphanage, and numerous shops were burned to the ground — lamenting, "People want news fast, and they could not wait, so they just went straight to Facebook."[15]

CHANGE IS (SUPPOSEDLY) COMING

It is undeniable that the use of social media in Myanmar has increased noticeably since the country re-opened itself to the world. At the beginning of July 2013, the government announced that it intended to increase

the percentage of mobile phone users, which as of 2013 stood below ten per cent, to eighty per cent by 2016. This came a week after the government awarded Norway's Telenor and Qatar's Ooredoo the first foreign telecommunications licenses in Myanmar.[16] Should these companies fail to live up to their fifteen-year license agreements, they will be required to pay US$200 million.[17] However, these companies will also be competing with two majority state-owned telecom entities, Myanmar Posts and Telecommunication (MPT) and Yatanarpon Teleport (YTP), which currently dominate the mobile market.[18] Ooredoo started selling its SIM cards in some of Myanmar's larger cities, such as Yangon and Mandalay, in August 2014. However, the network does not cover rural areas, leaving most communities unaffected by the new sales.[19] Meanwhile, Telenor's sales are expected to begin in September 2014 and would have a greater focus on rural connectivity.[20]

The telecommunications situation is made all the more precarious by a recent Telecommunications Bill that was passed by the Parliament in August 2013 and signed into law by the President in October 2013,[21] allowing the nation's mobile licensees to commence operations. Section 76 of the law continues to give the Ministry of Information and its related departments permission to inspect and "supervise" telecom providers. Sections 77 and 78 state that the government can intercept any data transmission or any communication that could compromise national security or the public order.[22] The government can also call on the telecommunications company to suspend its services altogether.[23]

Disconcerting legal measures extend to the print media as well. At the beginning of July 2013, Myanmar's Lower House of Parliament approved a version of the Printing and Publishing Enterprise Bill, which would effectively replace the 1962 Printers and Publishers Registration Act that had mandated pre-publication censorship, among other draconian measures. This controversial bill had undergone several previous iterations. In March 2013, the Ministry of Information (MoI) unveiled the original draft, which the Interim Press Council — a government-appointed group of mainly practising journalists and a retired Supreme Court judge — immediately condemned.[24] Among other concerning measures, the bill would forbid any criticism of the 2008 military-drafted Constitution and would give the Ministry of Information broad powers to issue and revoke pub-

lishing licences. The Myanmar Journalists Association, the Myanmar Journalists Network, and the Myanmar Journalists Union protested against the bill, as the Ministry of Information had failed to consult with media stakeholders prior to the production of the draft law. As a result, the Interim Press Council submitted its own Press Bill for consideration, outlining the rights and obligations of the media and advocating self-regulation.[25]

In November 2013, the Lower House of Parliament agreed to abolish prison sentences altogether for printing or publishing without registration and reduced the financial penalty from 10 million kyat (roughly US$10,300) to a maximum of 300,000 kyat (around US$300). The prohibition against criticizing the 2008 Constitution was also removed. However, the bill still bans the publication of material that "insults" religion, expresses nudity, undermines the "rule of law" or harms ethnic unity.[26] U Ye Htut, the Deputy Minister of Information and spokesman for the President, responded to criticism of the bill on his Facebook page, writing that "this law has nothing to do with controlling press freedom."[27]

In March 2014, Myanmar's Parliament approved the two media laws — the journalists-drafted Press Law and the Ministry of Information's own Printing and Publishing Enterprise Law — with the government still affirming that these pieces of legislation would increase press freedom, despite leaving media licensing in the hands of the Ministry of Information. For a sense of perspective, a year and a half earlier, the Myanmar government formally ended its pre-publication censorship system, which resulted in the dissolution of the country's infamous Press Scrutiny and Registration Division (PSRD). Then in April 2013, Myanmar saw the publication of its first private daily newspapers in nearly five decades. Now some thirty private dailies have been awarded licenses, although they have struggled to compete with state-run media.[28] Aside from these measures, Myanmar has been slow in enacting tangible legal reforms. The infamous Electronic Transactions Law — which allows for prison terms ranging from seven years to fifteen years for receiving or sending information over the Internet that was deemed to be a threat to state security or national solidarity — remains in place.[29] The Public Service Media Bill, which would regulate Myanmar's state-run newspapers, radio stations, and television channels, proposes to continue the state funding of these entities.[30] Meanwhile, private

businesses would be barred from simultaneously operating both broadcast and print media.

Implementing legal safeguards that protect freedom of speech and access to information are fundamental to creating a culture of democracy and justice. The country is at a difficult juncture, trying to pursue political and economic reforms while numerous ethnic and religious conflicts — namely the Buddhist-Muslim divide, in the context of this chapter — continue to flare. The government should not view freedom of information as the end goal of the country's democratization but rather as an integral element of the country's transition. The vituperations and racial slurs, while shameful, reflect underlying ethnic and religious tensions that cannot be overlooked if a genuine democratic transition is to be achieved. The next section shall trace the religious conflict between Buddhists and Muslims that has been spreading around Myanmar since June 2012, and shall document the manner in which the government has tried to control the country's access to information — in some ways subtly and in other ways more overtly — in order to, rather ineffectively, quell tensions.

THE MUSLIM-BUDDHIST DIVIDE COMES TO THE FORE

On May 28, 2012, a 26-year-old Buddhist woman named Ma Thida Htwe was gang-raped and murdered, allegedly by three young Rohingya Muslim men in Rakhine state (formerly known as Arakan state). A few days after the murder, photographs of the victim were circulated on Facebook. Photos of three men identified as the rape suspects were also published. These photos were then widely shared on the Internet. A weekly journal, *Snapshot* (*Hlyat Tabyet* in Myanmar), published a picture of the victim's corpse, which stoked outrage among the population. The now-defunct PSRD temporarily suspended *Snapshot* for printing inflammatory material. Six days later, on June 3, 2012, a mob of 300 Buddhist Arakanese stopped a bus, dragged out ten Muslim pilgrims — who were not in fact ethnic Rohingya — and beat them to death in the town of Taungup.[31] Some Internet users posted pictures of the slaughter on their Facebook accounts and other public media sites, calling many of the victims "kalars", a derogatory term for someone from South Asia with dark skin. On June 5, state-run newspapers the *Mirror* (*Kyemon*) and the *New Light of Myanmar* (*Myanma Alin*) also used the term "kalar". Meanwhile, independent *Eleven Media* group and the *Voice Weekly* referred to the Rohingya as "terrorists".

The Facebook pages of these media outlets had readers posting equally acerbic comments.[32]

These incidents precipitated an outbreak of violence throughout Rakhine State. On June 8, thousands of Rohingya Muslims rioted in the town of Maungdaw, destroying Arakan Buddhists' property and causing an unknown number of deaths. In turn, Arakanese groups, sometimes with the support of local authorities and the police, rioted against Rohingya communities, culminating in killings, beatings, and the burning of Muslim homes and villages.[33] Tens of thousands of individuals, primarily Rohingya, were displaced as a result, and a year later, in July 2013, that number was estimated to have swelled to the hundreds of thousands.

HISTORY OF THE ROHINGYA IN MYANMAR

These tensions are not new. Many Rohingya say that their origins can be traced back to the eighth century when the first Arab Muslims arrived in Rakhine State as traders, although some historians deny that there is any connection between the early Arabs and the Rohingya. In the fifteenth and sixteenth centuries, present-day Rakhine State was an independent principality and home to both Buddhists and Muslims. During British colonial rule, tens of thousands of migrants from British India, which included present-day Bangladesh, were brought in to work in the local paddy fields.

The term Rohingya is thought to have emerged in the 1950s. Nevertheless, what are now called Rohingya in the media are still commonly called "Bengalis" by the Myanmar population. The word Rohingya cannot be found in the nineteenth century British censuses, which counted nearly 60,000 Bengalis as living in Rakhine province by the end of the century. By 1911, the population had increased to 178,647.[34] After General Ne Win's 1962 coup d'état, the population was subjected to recurring targeted military operations. Perhaps the most prominent operation was Operation Naga Min ("Operation King Dragon") in 1978, which resulted in over 200,000 Rohingya fleeing to Bangladesh as refugees.[35] Less than three years later, the Myanmar government passed the 1982 Citizenship Act, which effectively denied citizenship to the Rohingya. The 1983 census counted the Rohingya as foreigners, and the Minister of Population and Planning in charge of supervising the national census in 2014 said that

there were still no plans to change their status.[36]

Now, approximately thirty years after the 1982 Citizenship Act was passed, between 800,000 to one million Rohingya remain stateless in Myanmar and are thereby denied fundamental rights, not the least of which is a right to a nationality as outlined in Article 15 of the Universal Declaration of Human Rights.[37] However, while the Myanmar government has a history of maltreatment of ethnic minorities that it deems to be citizens, the Rohingya's lack of citizenship provides an even easier pretext for the government's failure to protect this population's rights and commit egregious human rights transgressions. The Rohingya are subjected to forced labour, arbitrary land seizure, and excessive taxes. There are also restrictions on marriage and the number of children that Rohingya can have.[38] However, it should be noted that the ethno-religious violence in Myanmar has spread such that the country's Muslim population at large, not just the Rohingya, has become the target.

President Thein Sein, and even Nobel Laureate Daw Aung Saw Suu Kyi, not wanting to ruffle the feathers of the administration or the majority-Buddhist population, have avoided addressing the issue directly, despite regional and international expressions of concern. In an effort to diffuse tensions and stymie the spread of inflammatory coverage and commentary, the government has tried to manipulate the media and the media's access to the conflict regions. The government has, in effect, reasserted its control of the media and expunged new-found media freedoms. Despite the dissolution of the PSRD and the licensing of private news dailies, the government has tried to promote a culture of self-censorship while failing to take any substantive action in addressing the ethno-religious issues.

WHEREIN LIES THE MEDIA REFORM?

While Myanmar news organizations were able to access the towns in Rakhine State where the earliest clashes took place, foreign news agencies only began arriving after June 8, 2012, according to Reporters Without Borders.[39] Reporters were then repeatedly met with pressure from the local population in terms of how to represent the violence or whether to publish the events at all, such that many reporters found themselves returning to Yangon in order to file their stories. Many local reporters —

either working for domestic media outlets or as stringers for international media organizations — found it difficult to separate their own entrenched feelings about the Rohingya population from their reporting work.

Then, for the first time since taking office in March 2011, U Thein Sein declared a state of emergency in Rakhine State on June 10, 2012, authorizing troops to take control of the region in the name of restoring law and order. During a press briefing that day, Yangon Division Chief Minister Myint Swe warned journalists to be careful when reporting on the Rakhine unrest. He asked for the media not to use inflammatory language that could lead to further instability, warning that those failing to do so would be charged with section 5(j) of the Emergency Provisions Act and Section 505(b) of the Myanmar Penal Code — resulting in up to nine years in prison.[40] According to section 5(j) of the Emergency Provisions Act,[41] any actions that aim to "affect the morality or conduct of the public or a group of people in a way that would undermine the security of the union or the restoration of law and order" are punishable by up to seven years in prison and/or a monetary fine.[42] Under Section 505(b) of the Penal Code, any action "with intent to cause, or which is likely to cause, fear or alarm to the public or to any section of the public whereby any person may be induced to commit an offence against the state or against the public tranquillity" is punishable by up to two years in prison and/or a fine.[43] Tint Swe, deputy director-general of the PSRD censorship body, which was still operating at the time, told those in attendance that all news would have to pass through his department before publication, reaffirming the censorship board's strong role. Rather than trying to clarify what had been occurring in the region, the government used the June 10 press conference as a means to intimidate the media. An actual overview of the situation in Rakhine state would come five days later, when the government convened yet another press conference in which it informed the media about the state of emergency and the curfew imposed on some of the cities in the area.[44]

Nevertheless, the sincerity of the government's media demands was made quite clear when the government suspended the weekly *Snapshot* for publishing a photo of the aforementioned rape victim.[45] *Snapshot* editor U Myat Khine noted in an interview with the *Irrawaddy* that since the photo had already been circulating online for days he thought that there was

nothing wrong with publishing it; thereby illustrating a failure to distinguish between social media fodder and more professional reporting.[46] To date, the original source, or sources, of the photos containing the rape victim's lifeless body and the rape suspects is, or are, still unknown.

Meanwhile, the Internet in Myanmar became a hotbed of virulent smear campaigns and malignant social organizing. A series of online campaigns were launched to coordinate attacks on news outlets that were deemed to be showing sympathy toward the Rohingya's plight. Demonstrators rallied in Yangon in June 2012, condemning such news outlets as the *BBC* and the *Democratic Voice of Burma* (*DVB*), with some enraged protesters calling the former the "Bengali Broadcasting Corporation" and the latter the "Democratic Voice of Bengali". Protesters brandished signs stating: "International media STOP stating this as RELIGIOUS conflict" and "Rohingya is NOT Myanmar ETHNICITY".[47]

There are numerous reasons why these demonstrations were alarming. For one, these demonstrations reflected the population's endorsement of the government's decision to limit the news coverage of the ethno-religious conflict. Secondly, these protesters were advocating for censorship of the very same media outlets that in many ways had long sought to give the Myanmar people a voice.[48] Some of the news outlets that protesters were demonstrating against used to be revered as the few reputable media outlets providing news for the country. For instance, the *DVB* — which maintains a radio service, online news content, and a television channel — was founded by Myanmar exiles operating out of Norway and Thailand. The organization used stringers to collect information inside Myanmar and continued to publish its news — along with rather unvarnished critiques of the government — from abroad until 2012, when the *DVB* decided to launch an office inside Myanmar.

On June 9, 2012, the *DVB* website also faced a distributed denial-of-service (DDoS) attack,[49] and its Facebook page came under assault from people issuing threats and posting racially-tinged comments. According to the *DVB*, approximately five hundred computers were used to attack the English and Myanmar versions of its website.[50] A group of hackers calling themselves "Blink" claimed responsibility for the attack and encouraged others to follow suit. An analysis of the origin of the IP addresses used in the DDoS attack showed that at least seventy-five of them were from Rus-

sia or Singapore. Similar attacks targeting Myanmar-exile media groups occurred in 2008 and 2010, on the anniversary of the September 2007 anti-government protests that were violently quashed by the military.[51]

There has also been speculation that information in the news and on social media has been manipulated by the Myanmar government and/or the military — the two of which are still very much intertwined — with the aim of actually stoking ethno-religious tensions and establishing a situation in which it is necessary for the military to step in as the only suitable guarantor of public order and security.[52] It seems unlikely that what has now become a national ethno-religious conflict was premeditated, as the country already has numerous other ethnic conflicts to contend with.[53] However, a number of questions remain unanswered — perhaps most notably, how the photos of the rape victim and her supposed aggressors were made available to the general public and circulated so quickly. The three suspects were arrested on May 30, 2012, just two days after the incident. The provincial court sentenced two of the three suspects to death on June 18, 2012, and the third suspect allegedly took his own life before the sentence was given.[54]

PATTERNS EMERGE: THE MEIKHTILA MASSACRE

As the ethno-religious violence has spread throughout the country, a few patterns have emerged. For one, the media's access to the conflict areas was heavily constrained, by both the government and the local communities. Secondly, Muslim individuals involved in the violence were repeatedly convicted more readily than Buddhist transgressors.

When violence erupted on March 21, 2013, in Meikhtila — located in the central Myanmar province of Mandalay, not far from the Masoeyein Monastery of U Wirathu's 969 movement — the constraints and threats placed on the media seemed to be just as severe, if not worse, than those experienced in Rakhine state. Clashes broke out following a quarrel between a Buddhist couple and the Muslim owner of a goldsmith shop, and a separate incident in which a Buddhist monk was burned to death by four Muslim men. The monk's death stirred emotions in Meikhtila after photos circulated widely through social media of what was purported to be his body. Buddhist mobs torched the Himayathul Islamic Boarding School, slaughtering thirty-two students and four teachers, and went on to

burn down Muslim businesses and all but one of the city's thirteen mosques. The violence quickly spread to other towns in the region and raged for more than a week, leaving at least forty-four dead and 12,000 displaced — most of them Muslims.[55]

News from what has been deemed a "massacre," was slow to trickle out due to vociferous threats from monks and other anti-Muslim mobs targeting journalists. According to a report by the Committee to Protect Journalists, journalists working for local and foreign news agencies and outlets — such as the Associated Press (AP), Agence France-Presse (AFP), Radio Free Asia, *Democratic Voice of Burma* (*DVB*), and the *Irrawaddy* — were confronted by armed mobs, trying to block them from reporting on the riots.[56] In one incident, a group of armed Buddhist monks threatened nine journalists who were photographing the monks as they damaged a mosque.[57] The Associated Press reported that a monk placed a foot-long dagger at a reporter's throat and demanded that he hand over his camera, at which point the reporter surrendered his camera's memory card.[58] A *DVB* reporter was threatened by rioters wielding swords and was forced to delete his footage. A photographer for the *Irrawaddy* was forced to delete photos that had been taken of the casualties and damage.[59] While no journalists were reportedly killed or seriously injured, some decided to leave the city, concerned that authorities were not providing enough security.[60]

The most detailed account of the Meikhtila massacre did not emerge until the beginning of July 2013, when the AP published a piece that collated ten eyewitness accounts, including seven from individuals who had survived severe injuries. According to the AP, these accounts were then verified by assessing video clips taken by private citizens (many with embedded metadata like date and time being present), public media footage, dozens of photos, a site inspection of the Himayathul Islamic Boarding School, and information from local officials.[61] Due to security concerns, the eyewitnesses requested that they be interviewed at a local hotel rather than at their homes.

As was later disclosed in another AP article published on July 29, 2013, when a team of AP reporters went to Meikhtila to conduct the interviews and assess the destruction, they were hounded by intelligence agents. On the way to the hotel, the journalists realized that two men were trailing be-

hind them on motorcycles. Then other agents were waiting outside of the hotel. Trying to find a way to lose them, the reporting team ultimately decided to enter a crowded temple and slipped out the back.[62]

During the days of the military regime, being trailed by intelligence agents and police officials was all too common. Even now, journalists, political figures, and humanitarian workers still find themselves being watched. It is unknown how many intelligence agents are still active around the country, but at least two major information gathering services are still in operation: the Office of Military Affairs Security and the infamous Special Branch Police, which reports to the Ministry of Home Affairs.[63]

Deputy Information Minister Ye Htut, who is also the presidential spokesperson, has denied that agents still monitor journalists.[64] However, it is evident that the practice still exists on a nationwide scale, and the local police also continue to employ their own intelligence agents.[65] When a team of AP reporters visited a Muslim neighbourhood in Sittwe, the capital of Rakhine state, after the ethno-religious violence there, half a dozen police carrying assault rifles followed the reporting team for the entire trip and jotted down everything they heard in notebooks. Police officers also appeared during interviews at camps for internally displaced persons and asked journalists whom they had spoken with and what questions they had asked.[66]

What was perhaps most disturbing, though, about the AP piece on the Meikhtila massacre was the revelation that victims, particularly those at the Islamic boarding school, were slaughtered before the very eyes of police and local officials who, for the most part, stood by and failed to intervene. The government did not reprimand the police for their failure to protect the community. However, just as in the case of the Rakhine state violence, the government declared a state of emergency on March 22, 2013, effective not only in Meikhtila, but also in Mahlaing, Wundwin and Thazi, to which regions the violence had spread.[67] While conveying the news of the declaration of emergency, state-run television said that "local security forces and authorities have to seek military help to restore order effectively," suggesting that the government would use the military to suppress the ongoing riots.[68] While Meikhtila is home to the Myanmar Air Force's central command, the Meikhtila air base and the Myanmar Army's 99th Light Infantry Division, the military had not exerted any major effort to

end the violence there before martial law was declared.[69]

Much as in the case of the Rakhine state violence, the first people prosecuted for the violence in Meikhtila were not those from the Buddhist mobs, but rather the Muslims. On April 11, 2013, a Meikhtila court sentenced the Muslim gold shop owner and two employees to fourteen-years in jail for theft and for causing grievous bodily harm. On May 21, the same court sentenced seven Muslims to terms ranging from two years to life for their roles in the killing of the monk on March 20.[70] It was not until July 10, 2013, a few days after the AP piece came out, that the first Buddhists were sentenced for their actions during the massacre. Seven Buddhists received sentences for between three and fifteen years, rather incongruous sentences, given that some were found guilty of murder. These sentences were dealt just a day after yet another Muslim man was sentenced to life in prison for the killing of a university student in Meikhtila.[71]

THE BLAME GAME

The state of emergency remained in place until July 20, 2013, when President Thein Sein was completing a European tour — the first by a Myanmar president in forty-six years — that was aimed, at least in part, at restoring the country's image in light of the ongoing violence. According to an article in the *New Light of Myanmar*, a state-run newspaper, the decision to lift the emergency order several months ahead of schedule in the four Mandalay townships was an indication that "peace and stability" had been restored. U Thein Sein told the France 24 news channel that allegations of "ethnic cleansing" were not true and were part of a "smear campaign" by outsiders.[72]

U Thein Sein's rhetoric of blaming unidentifiable outsiders sounds not all that unlike how 969 leader, U Wiratha, has repeatedly blamed ambiguous "Islamic extremists" for the negative press and other threats that have targeted him.[73] Just two days after the state of emergency was lifted in the four Mandalay provinces, a bomb went off in central Mandalay while U Wirathu was giving a mass sermon.[74] U Wirathu again attributed the attack to Islamic extremists in an interview with the *Irrawaddy*, and cited a video titled "Mohamed is now asking for Wirathu and Pyinnyarwara. Who will bring them?" that was allegedly spreading online, containing a message against U Wirathu, his fellow monk U Pyinnyarwara, and the 969

movement.[75]

The connections between the government and the 969 movement do not end there. What is perhaps most disconcerting about that relationship is the manner in which the government has defended the 969 movement despite its vituperative language toward Myanmar's Muslim population. When President Thein Sein announced the ban on the *Time* magazine piece, in which U Wirathu was called "The Face of Buddhist Terror", the President issued a statement that failed to condemn U Wirathu for his actions, and instead made the announcement out to be more of a sweeping endorsement of the 969 movement. Below is the English version posted on the Office of the President's website, as well as on Facebook:

> U Wirathu, a son of Lord Buddha, appeared at the cover (*sic*) of the *Time* Magazine issued on 1 July 2013, Vol.182, No 1 with an article entitled The Face of Buddhist Terror. Myanmar is a country with freedom of religion without discrimination amongst various faiths . . . . Buddhism is a religion that teaches for noble peace based on the knowledge practiced (*sic*) by ourselves with the firm belief on one's own actions and its results. The members of Sangha, sons of Lord Buddha, have been peacefully and strictly following 227 kinds of Code of Conduct (Vinaya), striving for the purification, perpetuation and propagation of the Sasana for thousands of years. Moreover, the symbol 969 is known to represent nine virtues of Lord Buddha, six virtues of Dhamma and nine virtues of Sangha which is (*sic*) referred to as Three Gems that is (*sic*) deeply venerated by Buddhists as a symbol of peace . . . . Today, the Government is undertaking the transformation process to build an independent and transparent democratic society . . . . The article that appeared in Time Magazine not only misled many on Theravada Buddhism, the main belief of majority of Myanmar people which has been practised for thousands of years but also damaged the Government's efforts to build mutual respect amongst people of different religions. Thus, we reject the article "the Face of Buddhist Terror" written in the *Time* Magazine issued on 1 July 2013.[76] [paragraph divisions omitted

– Ed.]

MYANMAR'S A2K OUTLOOK

The ethno-religious violence between Muslims and Buddhists that has swept Myanmar since June 2012 could become one of the country's largest impediments to democracy. In looking at the situation from an access to knowledge (A2K) perspective, this conflict has elucidated a few issues that are particularly disconcerting. For one, it is quite clear that the country has yet to attain genuine media freedom. Not only is the government initiating measures that prevent journalists from reporting on the violence, but the local communities often appear equally complicit in limiting the news coming out of conflict areas. The fact that monks are commonly at the fore of both the violence and the threats against the media adds yet another layer of difficulty in addressing the press freedom issue. Monks garner an unparalleled amount of respect in Myanmar, as well as in other Buddhist countries. When individuals as revered as monks are stoking the very flames of violence that could lead to the country's undoing, this puts the government in a difficult position.

Another concern is that social media platforms are becoming popular in Myanmar concurrently with this public expression of hate speech, and, as a result, this scurrilous language is making its mark on social networking sites and colouring how they are used in the country. Surely the hate speech — and the sentiments that are fomenting such hate speech — already existed, but there is a possibility that these new means of expression could further augment existing ethnic and racial tensions. The violence is being both exacerbated by and reflected in these new channels of expression.

Deputy Information Minister and presidential spokesman Ye Htut suggested at the U.S. Embassy's June 2013 "hate speech" workshop, that one answer to the hate speech issue comes in better training local "media professionals" to produce fast, yet ethical, news that does not rely on hearsay but rather on well-researched and balanced reporting that pre-emptively stems the tide of sensationalist reports.[77] However, that is not the only answer. The government must also take greater responsibility in addressing the many human rights abuses associated with the conflict, including — but not limited to — the current "illegal" status of the Rohingya, the gov-

ernment's restrictions on humanitarian aid to the displaced communities, and the government's overt attempts at barring journalists from producing more candid, yet professional, accounts of the conflict.

At the behest of the international community, on August 17, 2012, President Thein Sein ordered a committee to investigate the causes of the violence and issue recommendations. However, the 'Inquiry Commission on the Sectarian Violence in Rakhine State' was composed of twenty-seven members mainly from local security forces and Rakhine state officials, putting into question the objectivity of the commission. The commission's findings, detailed in a report submitted to President Thein Sein in April 2013, were met with great criticism. The United Nations Special Rapporteur on the human rights situation in Myanmar, Tomás Ojea Quintana, expressed concern over the lack of recommendations to address impunity and to ensure comprehensive investigations into allegations of systemic human rights violations.[78]

The government's failure to address human rights violations and its efforts to bar reporting on such human rights violations are not solely confined to the violence originating in Rakhine state. Another example comes out of Kachin state, in northern Myanmar, where the government has been engaged in fierce fighting with the Kachin Independence Army (KIA), one of the many ethnic rebel groups in the country seeking greater autonomy. This decades-long civil war between the KIA and the Myanmar military resurged in January 2013 with the military introducing massive artillery barrages supported by air strikes from attack helicopters and fighter jets.[79] In February 2013, several journalists covering Myanmar received notifications from Google that their e-mail accounts may have been hacked by "state-sponsored attackers". Among those receiving the messages were employees of the Eleven Media Group; Bertil Lintner, an expert on Myanmar's ethnic groups; and a Myanmar-based correspondent for the Associated Press.[80] Many have speculated that these hacking attempts were linked to the conflict in Kachin state, as all of the journalists had reported on the armed conflict, despite official attempts to ban reporting in the area.[81] The *Weekly Eleven* was the first local publication to report in late December 2012 that government forces had used air power against rebel forces — news that ignited international condemnation.[82] In January 2013, Myanmar's Ministry of Defence condemned the international criti-

cism, declaring that international organizations, embassies, and the media were "fabricating news" about the Kachin conflict, again evincing the government's penchant for blaming outside sources rather than acknowledging what have become well-documented conflicts in the country.[83]

What is additionally troubling is that the country, while making ostensible media reforms, has been lagging in its codification of these reforms into law. The recently-passed Printing and Publishing Enterprise Law, the Public Service Media Bill, and other legislation are gaining support in the Parliament, yet these will in no way ensure media freedom, if they remain in their current forms. The government must clearly demarcate its role in the media scene, or rather, what should be a lack of a role, in whatever media laws are ultimately passed.

For now, Myanmar's press freedom gains appear tenuous at best. The government has imposed new restrictions on foreign journalists' visas, in some cases severely limiting the amount of time that foreign reporters can stay in the country. The Ministry of Information has also reduced the number of visas issued to journalists from formerly exiled media outlets, such as the *Irrawaddy* and *DVB*.[84] In April 2014, a *DVB* reporter was sentenced to one year in prison for allegedly trespassing and disturbing a civil servant while conducting an investigation into possible corruption in a local education department. Two months later, a provincial court sentenced the CEO and four reporters of a weekly newspaper to ten years in prison plus hard labour for publishing a report that indicated a large, clandestine government factory had been designed to produce chemical weapons.[85]

A government that is accustomed to maintaining state control over the media and telecommunications industries may have difficulty embracing all that freedom of the press and freedom of speech encompass. Myanmar is at a crossroads as it aims to enhance connectivity on a number of levels. The country aims to become both more regionally and globally integrated, while also attaining greater connectivity domestically among its own population. This is a tall order, particularly for a country that has been isolated from the international community for decades, lacks significant human and physical capital, and has over a quarter of the population living under the poverty line. Perhaps the greatest test will be the extent to which the government is willing to relinquish its control of the media and

telecommunications industries, while also ensuring that the population — and not just international investors — benefit from the country's reforms. As the international community becomes increasingly interested in Myanmar, this new-found interest should be used to ensure that the country moves toward veritable freedoms for the Myanmar people, and not just to pursue burgeoning business opportunities.

1 Editorial Note: This chapter will use the word "Myanmar," rather than "Burma," as the former has become increasingly accepted by the international community. The adjectival form of Myanmar can be "Myanma" or "Myanmar", and the latter is used in this chapter, while referring to the Myanmar people or the Myanmar government. Also note that 'U' in 'U Wirathu', is an honorific added to the names of older Myanmar men, as 'Daw' is an honorific added to the names of older Myanmar women. The 'U' is dropped when something else, such as 'President' is added to the beginning of the name in writing or speaking. Therefore, you will see both "U Thein Sein" and "President Thein Sein" in this text. Lastly, Myanmar individuals do not have specific first names/last names, so their full names are used throughout this text.

2 U Wirathu also stated in an interview with the *Irrawaddy*, an independent Myanmar newspaper, that Islamic extremists want his downfall and that is why he was put on the *Time* cover. *See Islamic Extremists Want My Downfall, That's Why They Put Me On The Cover*', IRRAWADDY (June 24, 2013), http://www.irrawaddy.org/archives/38277.

3 Shawn W. Crispin, *Online and in Danger in Burma,* COMMITTEE TO PROTECT JOURNALISTS (June, 13, 2013), http://www.cpj.org/reports/2013/06/online-and-in-danger-in-burma.php.

4 *Burma Bans Time Magazine's 'Buddhist Terror' Edition*, DEMOCRATIC VOICE OF BURMA (June 26, 2013), http://www.dvb.no/news/politics-news/burma-bans-time-magazine%E2%80%99s-buddhist-terror-cover-story/28973.

5 A period of reform has ensued since Myanmar's November 2010 presidential election, which brought U Thein Sein into power. The Union Solidarity and Development Party (USDP), the military's political entity, won a landslide victory and established a new "civilian government" the following March, the first civilian government in nearly 50 years. Headed by U Thein Sein, former prime minister of the military government, the USDP government effectively began as an extension of military rule, and then a series of rather unexpected top-down reforms were invoked in August 2011.

6 *Time Magazine Misinterpretation Rejected,* OFFICE OF THE PRESIDENT OF THE REPUBLIC OF THE UNION OF MYANMAR (June 23, 2013), http://m.president-office.gov.mm/en/briefing-room/news/2013/06/25/id-2257.

7 *See Time Magazine Censored Twice Over For Coverage of Radical Buddhists*, REPORTERS WITHOUT BORDERS (June 26, 2013), http://en.rsf.org/burma-time-magazine-censored-twice-over-26-06-2013,44860.html.

8 *Burma Bans Time Magazine's 'Buddhist Terror' Edition*, DEMOCRATIC VOICE OF BURMA (June 26, 2013), https://www.dvb.no/news/politics-news/burma-bans-time-magazine%E2%80%99s-buddhist-terror-cover-story/28973.

9 Ei Khine & Kyaw Thu, *Myanmar's Thein Sein Calls for Responsible Reporting from Media,* RADIO FREE ASIA (Khet Mar & Joshua Lipes, trans.) (July 2, 2013), http://www.rfa.org/english/news/myanmar/media-07022013182350.html.

10 Cherry Thein, *'Time' cover sparks outrage,* MYANMAR TIMES (June 24, 2013), http://www.mmtimes.com/index.php/national-news/7228-time-cover-sparks-outrage.html.

11 *Journalists Plan Protest against Media Restrictions,* IRRAWADDY (Aug. 17, 2012), http://www.irrawaddy.org/archives/11768.

12 President Thein Sein's reformist government approved a bill in early 2012 allowing authorized peaceful protests, but demonstrators must seek permission five days in advance.

13 Ei Ei Khine & Kyaw Thu, *supra* note 9.

14 *Id.*

15 Cate Cadell, *Govt Urges Journalist to Help Curb Hate Speech,* MIZZIMA (June 28, 2013), http://www.mizzima.com/news/myanmar/9602-govt-urges-journalists-to-help-curb-hate-speech.

16 Telenor and Ooredoo were selected from a pool of 11 global consortia. At least 91 companies and consortia had expressed interest in bidding for the two 15-year mobile licenses.

17 Ooredoo announced that it will take a 3G-only approach, "leapfrogging" all 2G technology. This approach will require accessibility to affordable 3G headsets, currently still beyond the financial reach of the general population, and more reliable power sources in Myanmar.

18 Moreover, it appears that other telecommunications companies that were not awarded the original licenses may become involved through other business arrangements. For instance, Singapore Telecommunications (SingTel), one of the losing bidders of the telephone network licenses, met with the Directorate of Investment and Company Administration (DICA) in Naypyidaw in October 2013 to discuss cooperation with Ooredoo and Telenor in network expansion and to help build Myanmar's satellite system.. Indonesia's PT Telkom meanwhile picked up the tender to manage Myanmar's international network connectivity, and the Japanese companies Sumitomo, NEC and NTT won a deal to enhance the nation's emergency communications infrastructure.

19Ooredoo has taken a 3G-only approach, leapfrogging all 2G technology. This approach requires accessibility to affordable 3G headsets, currently still beyond the financial reach of the general population, and more reliable power sources in Myanmar. Moreover, data packages are significantly more expensive than those currently offered by state-owned MPT.

20 Moreover, it appears that other telecommunications companies that were not awarded the original licenses may become involved through other business arrangements. For instance, Singapore Telecommunications (SingTel), one of the losing bidders of the telephone network licenses, met with the Directorate of Investment and Company Administration (DICA) in Naypyidaw in October 2013 to discuss cooperation with Ooredoo and Telenor in network expansion and to help build Myanmar's satellite system. Indonesia's PT Telkom meanwhile picked up the tender to manage Myanmar's international network connectivity, and the Japanese companies Sumitomo, NEC and NTT won a deal to enhance the nation's emergency communications infrastructure.

21 Telecommunications Law, Pyidaungsu Hluttaw Law No. 31, 2013 (Myanmar), *available at* http://www.mcit.gov.mm/content/telecommunications-law.html.

22 *Id.*

23 *Id.*

24 Zin Mar Win & Khin Khin Ei, *Myanmar's Press Council Opposes New Media Legislation,* RADIO FREE ASIA (July 5, 2013), http://www.rfa.org/english/news/myanmar/myanmar-07052013180935.html.

25 Thin Thiri, *Myanmar Parliament Passes First Legislation Granting Media Freedom*, RADIO FREE ASIA (Mar. 5, 2014), http://www.rfa.org/english/news/myanmar/media-03052014163116.html.

26 Ko Htwe, *Burma Amends Controversial Publishing Law,* DEMOCRATIC VOICE OF BURMA (Nov.

13, 2013), https://www.dvb.no/news/burma-amends-controversial-publishing-law/34369.

27 Simon Roughneen, *Burma's Press Council Threatens Resignation Over Media Rules,* IRRAWADDY (July 8, 2013), http://www.irrawaddy.org/media/burmas-press-council-threatens-resignation-over-media-rules.html.

28 However, publishers are still struggling to turn a profit, faced with the dominance of state-run media and a lack of advertising interest, and some publications have already been forced to shut down.

29 Shawn W. Crispin, *As Censorship Wanes, Cyberattacks Rise in Burma,* COMMITTEE TO PROTECT JOURNALISTS (Feb. 11, 2013), http://www.cpj.org/internet/2013/02/as-censorship-wanes-cyberattacks-rise-in-burma.php.

30 Public service (*i.e.*, state-run) media would receive seventy per cent of its funding from Parliament and thirty-percent from commercial sources such as advertising but would not pay taxes like other publications.

31 Kyaw Zwa Moe, *Why is Western Burma Burning,* IRRAWADDY (June 15, 2012), http://www.irrawaddy.org/commentary/why-is-western-burma-burning.html.

32 *Id.*

33 *Burma: Mass Arrests, Raids on Rohingya,* HUMAN RIGHTS WATCH (July 5, 2012), http://www.hrw.org/news/2012/07/05/burma-mass-arrests-raids-rohingya-muslims.

34 Aye Chan, *The Development of a Muslim Enclave in Arakan (Rakhine) State of Burma (Myanmar)*, 3 SOAS BULLETIN OF BURMA RESEARCH 396, 401 (2005), https://www.soas.ac.uk/sbbr/editions/file64388.pdf.

35 A similar operation in 1991, Operation Pyi Thaya (Operation Clean and Beautiful Nation), resulted in another 200,000 refugees fleeing to Bangladesh.

36 Danielle Bernstein, *Rights Group Presses Bangladesh on Rohingya Refugees*, VOICE OF AMERICA, June 20, 2012, http://www.voanews.com/content/rohingya-bangladesh-burma-myanmar/1216044.html.

37 Universal Declaration of Human Rights, G.A. Res. 217A (III), U.N. GAOR, 3d Sess., U.N. Doc. A/810 (Dec. 10, 1948).

38 *Burma: Rohingya Muslims Face Humanitarian Crisis,* HUMAN RIGHTS WATCH (Mar. 26, 2013), http://www.hrw.org/news/2013/03/26/burma-rohingya-muslims-face-humanitarian-crisis.

39 Benjamin Ismaïl, *Crisis in Arakan State and New Threats to Freedom of News and Information,* REPORTERS WITHOUT BORDERS (June 28, 2012), http://en.rsf.org/burma-crisis-in-arakan-state-and-new-28-06-2012,42908.html

40 *Press Warned Against Inciting Arakan Clashes,* IRRAWADDY (June 11, 2012), http://www.irrawaddy.org/censorship/press-warned-against-inciting-arakan-clashes.html.

41 In August 2011, a motion in the Lower House to repeal the 1950 Emergency Provisions Act, which has been used for decades to imprison democracy activists, was overwhelmingly rejected by the majority opposition dominated by the military-backed USDP. This was reaffirmed in July 2013, when the Deputy Home Affairs Minister, Kyaw Kyaw Htun, said during an address to Parliament that there was no need to amend the 1950 Emergency Provisions Act.

42 *Section 5 of the Emergency Provisions Act*, ONLINE BURMA/MYANMAR LIBRARY (unofficial trans.), http://www.burmalibrary.org/docs6/Section_5_of_the_Emergency_Provisions_Act-en.pdf

43 *Myanmar: The Penal* Code, ONLINE BURMA/MYANMAR LIBRARY (unofficial trans.), http://www.burmalibrary.org/docs6/MYANMAR_PENAL_CODE-corr.1.pdf.

44 Ismaïl, *supra* note 39.

45 *Id.*

46 Lawi Weng, *Journal Suspended for Publishing Photo the Sparked Arakan Riots,* IRRAWADDY (June 12, 2012), http://www.irrawaddy.org/censorship/journal-suspended-for-publishing-photo-that-sparked-arakan-riots.html.

47 Ismaïl, *supra* note 39.

48 Hanna Hindstrom, *The Freedom to Hate,* FOREIGN POLICY (June 14, 2012), http://www.foreignpolicy.com/articles/2012/06/14/the_freedom_to_hate.

49 A DDoS attack is an attempt to disable access to a website by overwhelming the site with information requests so that it cannot respond to regular traffic. The incoming traffic flooding the victim originates from multiple sources — potentially hundreds, or thousands, or more — effectively making it impossible to stop the attack simply by blocking a single IP address and making it difficult to distinguish between legitimate user traffic and attacker traffic.

50 *Hackers Target DVB Website,* DEMOCRATIC VOICE OF BURMA (June 11, 2012), http://www.dvb.no/news/hackers-target-dvb-website/22389

51 *Id.*

52 Ismaïl, *supra* note 39.

53 The country is currently trying to draft a national ceasefire agreement, to formalize the terms of thirteen separate ceasefires it has arranged with a variety of ethnic rebel armies.

54 Ismaïl, supra note 39.

55 Ei Ei Khine, *More Casualties as Violence Spreads in Myanmar's Shan State,* RADIO FREE ASIA (Khet Mar & Joshua Lipes, trans.) (May 29, 2013), http://www.rfa.org/english/news/myanmar/lashio-05292013183333.html.

56 *Journalists Threatened in Sectarian Violence in Burma,* COMMITTEE TO PROTECT JOURNALISTS (Mar. 25, 2013), http://cpj.org/x/53cb [hereinafter, *Journalists Threatened*].

57 Kyaw Zaw Win, *Armed Myanmar Monks Threaten Journalists in Meikhtila,* RADIO FREE ASIA (Win Naing, Khin Maung Nyane, & Parameswaran Ponnudurai trans.) (Mar. 22, 2013), http://www.rfa.org/english/news/myanmar/meikhtila-03222013191441.html

58 *Id.*

59 *State of Emergency Declared as Death Toll Rises in Meikhtila,* IRRAWADDY (Mar. 22, 2013), http://www.irrawaddy.org/burma/breaking-news/govt-moves-to-quell-violence-in-meikhtila.html.

60 *Journalists Threatened, supra* note 56.

61 Todd Pitman, *AP Impact: Massacre of Muslims in Myanmar Ignored,* ASSOCIATED PRESS (July 5, 2013), http://bigstory.ap.org/article/after-myanmar-massacre-no-justice-muslims-0.

62 Todd Pitman, *A Relic of Myanmar's Past, Internal Spying, Stays,* ASSOCIATED PRESS (July 29, 2013), http://bigstory.ap.org/article/myanmar-internal-spy-network-lives.

63 *Id.*

64 *Id.*

65 *Id.*

66 *Id.*

67 The state of emergency imposed a curfew from 10 P.M. to 4 A.M., and barred the assembly of more than five people.

68 *State of Emergency Declared as Death Toll Rises in Meikhtila*, IRRAWADDY (Mar. 22, 2013), http://www.irrawaddy.org/burma/breaking-news/govt-moves-to-quell-violence-in-meikhtila.html.

69 Aye Nai, *Martial Law declared in Meikhtila as mobs threaten journalists,* DEMOCRATIC VOICE OF BURMA (Mar. 22, 2013), http://www.dvb.no/news/martial-law-declared-in-meikhtila-as-mobs-threaten-journalists/27175.

70 Pitman, *supra* note 61.

71 Rachel Vandenbrink, *Seven Buddhists Jailed Over Meikhtila Islamic School Massacre,* RADIO FREE ASIA (July 11, 2013), http://www.rfa.org/english/news/myanmar/meikhtila-07112013181859.html.

72 Yadana Htun, *Myanmar Lifts Emergency Order in Riot-Hit Areas,* ASSOCIATED PRESS (July 20, 2013), http://bigstory.ap.org/article/myanmar-lifts-emergency-order-riot-hit-areas.

73 Zarni Mann, *Islamic Extremists Want My Downfall, That's Why They Put Me on the Cover*, IRRAWADDY (June 24, 2013), http://www.irrawaddy.org/protest/islamic-extremists-want-my-downfall-thats-why-they-put-me-on-the-cover.html.

74 Four people were injured and no one was killed.

75 Zarni Mann, *Wirathu Blames 'Islamic Terrorists' for Mandalay Explosion,* IRRAWADDY (July 23, 2013), http://www.irrawaddy.org/conflict/wirathu-blames-islamic-terrorists-for-mandalay-explosion.html.

76 *Time Magazine Misinterpretation Rejected, supra* note 6.

77 Ei Ei Khine & Kyaw Thu, *supra* note 9.

78 *Myanmar/Rakhine Commission: "Positive starting point but Government must address impunity-UN* expert, UN OFFICE OF THE HIGH COMMISSIONER FOR HUMAN RIGHTS (May 1, 2013), http://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=13280&LangID=E.

79 Bertil Lintner, *The Military's Still in Charge,* FOREIGN POLICY (July 9, 2013), http://www.foreignpolicy.com/articles/2013/07/09/the_militarys_still_in_charge.

80 *The Weekly Eleven* of the Eleven Media Group was the first local publication to report in late December 2012 that government forces had used air power against rebel positions -- news that sparked international condemnation.

81 Thomas Fuller, *E-mails of Reporters in Myanmar are Hacked,* N.Y. TIMES, Feb. 11, 2013, at A5, *available at* http://www.nytimes.com/2013/02/11/world/asia/journalists-e-mail-accounts-targeted-in-myanmar.html?_r=0.

82 *Id*.

83 Saw Yan Naing, *Intl Community 'Fabricates News,' Myanmar Military Says,* IRRAWADDY (Jan. 29, 2013), http://www.irrawaddy.org/z_kachin/intl-community-fabricates-news-burma-military-says.html.

84 *Burma: Repression Marks Press Freedom Day*, HUMAN RIGHTS WATCH (May 3, 2015), http://www.hrw.org/news/2014/05/03/burma-repression-marks-press-freedom-day

85 Thomas Fuller, *Myanmar Court Sentences Journalists to Prison and Hard Labor*, N.Y. TIMES, July 11, 2014, at A1, *available at* http://www.nytimes.com/2014/07/11/world/asia/myanmar-court-sentences-journalists-to-10-years-of-hard-labor-in-prison.html?_r=0

BRAZIL

CHALLENGES FOR FREEDOM OF SPEECH ONLINE

Mônica Steffen Guise Rosina & Alexandre Pacheco da Silva

INTRODUCTION

Among its many features, the Internet works as a catalyst for discourse in and between societies around the world, allowing a wide range of people to instantly send and receive information relatively unfiltered by traditional power structures. As American legal scholar Jack Balkin puts it, "the digital revolution makes possible widespread cultural participation and interaction that previously could not have existed on the same scale,"[1] encouraging us to think of the changes that the Internet has brought about in terms of salience, rather than novelty — in terms of enabling cultural and political participation on a larger scale than otherwise possible, rather than creating entirely new forms of cultural participation or interaction. [2] In turn, this enables citizens to have a voice and engage in national and international debates around issues that for various reasons may just not be addressed by traditional media in a transparent manner (if addressed at all).

In theory, the existence of such virtual spaces mean that anyone can create and influence public debate and discourse by uploading texts, photographs or videos to any of the numerous platforms that host user-generated content. We have seen potent examples of such use of platforms in recent political events around the globe. From protests in Iran, Egypt and

Brazil to political declarations in the United States, we are constantly reminded that the Internet is, indeed, an important tool for organizing, problematizing and disseminating information.

Having access to the Internet, however, may not be enough to make sure that information flows in an ideal manner. Influence on people's ability to communicate seems to be increasingly relevant when it comes to free speech battles. While the virtual environment provides massive potential for free speech to blossom,[3] its own existence poses a real threat to democratic interaction, as new digital technologies may be used to strengthen old forms of control.[4]

The debate over freedom of speech frequently revolves around the question of whether governments restrict the rights of citizens to express their political views through different types of media. People tend to believe that this is not an issue in Brazil, with the general perception being that the government respects freedom of speech in most traditional cases.

In this chapter we argue that online freedom of speech is under threat in Brazil, and that control over private Internet services has been one of the most effective ways to undermine this freedom. This has happened both through overreach by courts, using the traditional tools at their disposal — such as injunctions — as well as through control of intermediaries, which is the kind of 'new school' censorship,[5] which Kaminski and Prakash highlight in the opening chapter of this book: less obvious, outsourced, indirect. Because it is camouflaged and not called what it really is, such new school censorship goes unnoticed and is little debated in the mainstream media. However, it isn't new school censorship alone that is a threat to Internet speech. The case studies we discuss in this chapter show that new school censorship and old school censorship are not rivalrous, but indeed, can act in tandem and work in unison when it comes to stifling speech.

Recent decisions by courts have legally limited the ability of Brazilians to use social networks as platforms for political protest, and is a rising threat to free speech. We believe that the new possibilities of decentralized political expression allowed by virtual social networks represent a new dimension in politics. Understanding how Brazilian courts balance freedom of speech as a democratic value with values such as dignity and hon-

our is of utmost importance for the effective understanding of not only the possibilities afforded by virtual social networks, but also the way old school and new school censorship work.

The Brazilian Constitution, in the fundamental rights chapter states:

> *Article 5. All persons are equal before the law, without any distinction whatsoever, Brazilians and foreigners residing in the country being ensured of inviolability of the right to life, to liberty, to equality, to security and to property, on the following terms:*
>
> . . .
>
> *XI. The expression of intellectual, artistic, scientific, and communications activities is free, independently of censorship or license.*[6]

Moreover, as a response to the authoritarian military dictatorship that ruled the country from 1964 to 1985, the Constitution contains a special chapter on 'social communication', wherein article 220 states:

> *The manifestation of thought, the creation, the expression and the information, in any form, process or media shall not be subject to any restriction, with due regard to the provisions of this constitution.*
>
> *Paragraph 1: No law shall contain any provision which may represent a hindrance to full freedom of press.*
>
> *Paragraph 2: Any and all censorship of a political, ideological and artistic nature is forbidden.*

These are constitutional values, embedded in the very being of our young Brazilian democracy. We thus understand that freedom of speech translates into at least two different types of guarantees: (a) the right to freely express ideas, political points of view, and different forms of opinion, without the risk of being punished for defending or disseminating any specific idea; and (b) the ability of individuals and groups to build on each other's ideas, promoting and disseminating knowledge.

Free speech relies not only on the mere absence of old-school state censorship, but also on the existence and maintenance of spaces that enable information flows and communication to take place. Infrastructure such as social networks are among such spaces. Consider, for example, websites

like Facebook and Flickr: while on the one hand they merely host different media and materials, and links to content hosted on third-party websites; on the other hand, they are also online community platforms that allow people to communicate and pursue common interests and activities because of the tools they provide. Within such spaces, freedom of expression finds a fertile ground. But while these tools and spaces empower people to better communicate, they are also potential risks.

To illustrate how difficult the judicial elaboration of constitutional values is becoming in the information age, this chapter presents two cases in which a Brazilian court was asked to balance the protection of free speech with the preservation of an individual's image, honour and dignity. We will also examine some of the potential dangers inherent in those decisions, and the harms they could bring to online interactions, given that the restrictions they impose limit access to the digital infrastructure on a larger scale, threatening free speech.

THE RIGHT TO ACCESS SOCIAL NETWORKS

Cassius Abraham Mendes Haddad is a Brazilian lawyer. He lives in Limeira, a countryside town in the state of São Paulo, with 276,000 inhabitants. He is an independent attorney, working with a wide and diversified range of areas, from civil to criminal law. Before he became a lawyer in 2012, Mr. Haddad used to be a businessman.

In 2008, Mr. Haddad gathered a pool of investors to modernize the Limeira shopping mall, the largest in the region, but his plan failed. However, in the aftermath of that failed venture, Mr. Haddad came upon evidence that, according to him, showed that local municipal authorities were conspiring with some businessmen to pilfer public money from the municipality using the shopping mall's expansion as a reason. Mr. Haddad believed that this was the reason behind an expropriation proceeding that resulted in the condemnation and dispossession of houses from several families around the shopping mall, adding up to an area of 10,000 square meters. The municipality was set to donate this land — free of cost — to the shopping mall venture, as an incentive to new businesses in town.

Mr. Haddad also suggested that the reason for the Mayor of Limeira donating the land was his having received bribes from the businessmen

behind the shopping mall expansion. He argued that the condemnation process and donation of the real estate were flawed, as none of the businessmen involved in the venture lost any of their own property during the expropriation proceedings, even though some of them owned land in the areas that were subject to expropriation.

In 2010, Mr. Haddad felt he had gathered enough documents and witnesses to provide a sound basis for his accusations, so he sought out a public prosecutor, Luiz Alberto Segalla Bevilacqua, and requested him to file a lawsuit against the City Hall for misappropriation of public funds, bribery, conspiracy and other similar crimes. Mr. Bevilacqua, in the position of the public prosecutor, with jurisdiction to act in defence of the city's interests, believed that there was not enough evidence to sustain Mr. Haddad's allegations in a lawsuit, and dismissed the complaint. Outraged by that, Mr. Haddad appealed to the Prosecutors' National Counsel ("Conselho Nacional do Ministério Público"), challenging Mr. Bevilacqua's decision, but there too he was thwarted.

In 2012, Mr. Haddad became a lawyer and decided to file a lawsuit[7] accusing Limeira's mayor of misappropriation of public funds, conspiracy and bribery, challenging the validity of the contracts that were established during that time and questioning Mr. Bevilacqua's decision not to file a case back in 2008. When Mr. Bevilacqua learned about the lawsuit, he went to the local press to get his side of the story told. Mr. Bevilacqua accused Mr. Haddad of being a "political terrorist", and of lying and seeking public attention, and engaging in this vilification campaign due to a political interest in the next local elections.

In the following months, a Twitter account named "@cassiushaddad" was created and tweets started to pop up. Below are a few examples of the translated tweets:

— Dr. Luiz Alberto Segalla Bevilacqua is biased and supports corruption.

— As the old saying about corrupted prosecutors and judges goes: To my friends, everything; to my enemies, the law. Prosecutors and Judges of Limeira support corruption.

— I heard from someone that Dr. Bevilacqua said that he would finish me off. I challenge this low-class prosecutor to go ahead and do it.

Mr. Bevilacqua considered such tweets a direct attack on his honour as a prosecutor and his dignity as public figure in the city, and filed a criminal complaint. Mr. Haddad was charged with defamation.

In his defence, Mr. Haddad claimed he was not the author of the tweets. According to him, someone else had created the account, using his name. In turn, he registered the incident before the city's police and requested the account be deleted, which happened five days after his complaint. If the story were to end here, this would be just another ordinary defamation case.

But the prosecutor in charge of the criminal complaint against Mr. Haddad requested the Criminal Court of Limeira to grant an injunction preventing Mr. Haddad from accessing all social networks available on the Internet, as a means of forestalling him from speaking out online against Mr. Bevilacqua. And even though the dispute arose because of a Twitter account, the prosecution requested the court to explicitly declare several social networks to be off-limits for Mr. Haddad — Facebook, Twitter, Orkut, MySpace, Flixster, Linkedin and Tagged — even though Mr. Haddad was not even a registered user on most of the social network listed by the prosecutor, having accounts on only Facebook and Twitter.[8]

The decision of the criminal court judge, Henrique Alves Correa Iatarola, is priceless, to say the least: not only did he grant an injunction barring Mr. Haddad from multiple social networks, he additionally ordered the defendant to report all his online activities to the court every month.[9] The court didn't stop there: it also required all the social networks cited in the case to produce monthly reports about the status of Mr. Haddad's accounts (and, presumably, non-accounts) and send them to the court.[10]

Under Brazilian criminal law, failure to comply with the terms of such an injunction could be seen as contempt of court, and subject the defendant to imprisonment. In other words, Mr. Haddad could be sent to jail for simply logging into his Facebook account.

THE RIGHT TO PROTEST ONLINE

Ricardo Fraga de Oliveira is an agronomist and a lawyer in the state of São Paulo. He works for the Environmental Department São Paulo Muni-

cipality and lives in a neighbourhood called Vila Mariana.

In June 2011, Mr. Oliveira started a social movement called O Outro Lado do Muro — Intervenção Coletiva ("The Other Side of the Wall — Collective Intervention"), which sought to foster debate about the role of property developers and large construction projects in the city of São Paulo. In one intervention, Mr. Oliveira set up ladders outside a few construction sites and invited pedestrians to look in and leave their impressions on a blackboard, along with their impressions of what would an ideal city should be like. This initiative brought together a number of concerned citizens who together chose some real estate ventures to monitor.

One of Mr. Oliveira's main concerns was a specific venture located at Conselheiro Rodrigues Alves Street in São Paulo, which was to be built by Construtora Mofarrej Vila Madalena SPE Empreendimentos Imobiliários S/A (hereinafter "Mofarrej"). The land on which the venture was to be located was deemed a residential area for over fifty years, due to environmental issues — a stream flows in the property — but Moffarej had obtained a licence to build a business centre there.

Mr. Oliveira and fellow activists started to investigate the reasons why a licence to build a commercial venture on land with environmental issues was granted in the first place. The group was able to obtain official documents and talk to a few city officials, which led them to believe that the licence was granted pursuant to the payment of a bribe by Mofarrej.

After the investigation, Mr. Oliveira organized a series of protests that took place outside the construction site, and also created a Facebook page to mobilize against the venture and against Mofarrej. Through Facebook, he explained the case, provided details about the investigation and the documents collected, and encouraged people to engage in a debate about the city, in their neighbourhood, as well as that particular Mofarrej venture. Mr. Oliveira also succeeded in gathering five thousand signatures to request the licence be reviewed. The initiative was so big that not-for-profit organizations, such as Movimento Defenda São Paulo, offered to help with further investigations and with rallying.

In March 2013, fearing the outcome of the protests and the potential damage to its image, Mofarrej filed a tort lawsuit against Mr. Oliveira, asking for compensation and the immediate termination of the mobilization

operations, both physically and on Facebook. The company explicitly requested an injunction preventing Mr. Oliveira from posting any comments regarding the venture or Mofarrej on Facebook during the entire course of the lawsuit.

The injunction was granted, and failure to comply subjects Mr. Oliveira to a daily fine of R$10,000 (roughly US$ 4,000).[11] Mr. Oliveira is currently fighting the court order.

WHY WE SHOULD ADDRESS INTERNET CENSORSHIP

Jack Balkin presents five characteristics of Internet speech that enhance democratic culture in modern societies.[12] First, speech on the Internet ranges over every possible subject and mode of expression (serious to frivolous), reflecting popular taste and opinions.[13] Second, the Internet, taken as a whole, is full of innovation, enabling people to develop new technologies, business models, structures of communication, etc., and these are key to changes in the ways that individuals interact with each other.[14] Third, the creativity depends on the ability to build on what has come before and the Internet a boon for that. The very nature of HTML code, Balkin points out, stimulates copying, imitation and linking.[15] Fourth, Internet speech is participatory and interactive. People are not passive, as compared to radio or television. Rather, they go online and search, publish new content, and discuss both serious and frivolous issues. Internet speech is, thus, a social activity that involves exchanging experiences and actions between users.[16] And fifth, the Internet allows people to create communities, cultures and subcultures.[17] It is freedom of speech that enables us to build these communities, to participate in the formation of culture, to engage in public discourse and debate, all of which in turn shape us as individuals. Internet speech is thus not only a part of an "interactive cycle of social exchange, and social participation", but also vital as part of an individual's self-realization.

If we accept these characteristics mentioned by Professor Balkin as true values, which we do, there are further and more severe consequences to court decisions such as the ones we present here. A lawsuit in Brazil could take years to be settled. Over those years, both Mr. Haddad and Mr. Oliveira will face harsh restrictions in their right to access and use social networks, which, needless to say, are most certainly not meant solely for the

purpose of political protesting, but also as a way for interacting with friends and family, commercial advertising, and a myriad of other purposes. Virtual spaces are increasingly crucial to human interaction as a whole.

In both cases we describe here, the rulings show that courts are not ready to deal with the Internet. Not only judges show lack of understanding of the purposes of different networks and, consequently, their potential for harm; but they also disregard the Internet as a legitimate space for the exercise of free speech.

Two questions come to mind: (a) is there a less drastic way for courts to limit the potential harm to plaintiffs' image and dignity?; and (b) if we don't fight these legal restraints, which ignore the values embodied by the way people are using the Internet today for political engagement and empowerment, wouldn't we be missing on the development of a new culture of democracy in Brazil: a digital democracy?

Both court decisions seem to harbour a narrow vision about the benefits of enhancing Internet speech as a tool for the growth of democratic culture and seem to adopt a very conservative approach when it comes to balancing the right of free speech and the protection of the honour and dignity of individuals. Because they restrict communications and social participation, don't these recent developments point to a new form of censorship?

These questions lead us to an interesting insight into the Brazilian model of democracy. The judiciary, which is usually perceived as a safeguard against acts of censorship by the executive, is, in this case, the very organ of the state that is silencing people.

1 Jack M. Balkin, *Digital Speech and Democratic Culture: A Theory of Freedom of Expression for the Information Society, 79* N.Y.U. L. REV. 1, 2 (2004).

2 *Id*.

3 *See* Balkin, *supra* note 1, at 3 ("Freedom of speech allows ordinary people to participate freely in the spread of ideas and in the creation of meanings that, in turn, help constitute them as persons. A democratic culture is democratic in the sense that everyone — not just political, economic or cultural elites — has a fair chance to participate in the production of culture, and in the development of the ideas and meanings that constitute them and the communities and sub-communities to which they belong.").

4 *See* Yochai Benkler, *Freedom in Systems*, 127 HARV. L. REV. F. 351, 355 (2014), (concurring with Jack Balkin, *infra* note 4, that "the very systems that enable new forms of speech also enable new forms of surveillance and censorship, and vice versa.").

5 *See generally* Jack Balkin, *Old-School/New-School Speech Regulation*, 127 HARV. L. REV. 2296 (2014), *available at* http://harvardlawreview.org/2014/06/old-schoolnew-school-speech-regulation/.

6 República Federativa do Brasil Constituição tit. II, ch. 1, art. 5, *translation available at* http://english.tse.jus.br/arquivos/federal-constitution.

7 T.J.S.P., Ação Pop. No. 24.2012.8.26.0320.

8 The injunction request shows that the prosecutor failed to acknowledge the different purposes served by each social network and the consequent potential (or lack of potential) for damage Mr. Bevilacqua's image. For instance, in the case of a music-oriented social network, like MySpace, the risk of damage to Mr. Bevilaqua's image and dignity is practically non-existent.

9 T.J.S.P., Rep. Crim. No. 3002031-98.2013.8.26.0320, Juiz de Direito: Henrique Alves Correa Iatarola, 04.04.2013, (on file with the authors).

10 *Id*.

11 T.J.S.P., Proc. Ord. No. 1008543-15.2013.8.26.0100, Juiz de Direito: Adilson Aparecido Rodrigues Cruz, 25.10.2011, T.J.S.P.J., *available at* http://esaj.tjsp.jus.br/cpo/pg/show.do?processo.codigo=2S0007V4O0000&processo.foro=100.

12 Balkin, *supra* note 1, at 31–32.

13 *Id*. at 31.

14 *Id*.

15 *Id*.

16 *Id*. at 32.

17 *Id*.

EGYPT

BEHIND EGYPT'S COMMUNICATION OUTAGE OF 2011

Censorship and Economic Liberty

Nagla Rizk[1]

INTRODUCTION

In January 2011, the Internet and cellular telephone networks in Egypt went dark. The decision to sever communication was taken by the Egyptian government under then-President Hosni Mubarak in the context of a political uprising directed against the regime. While the political implications of the blackout have received some due attention, two angles still remain un-ventured: first, how the infrastructural set-up aided the implementation of the order, and second, an analysis of the economic implications of this censorship.

In this chapter I try to fill a void in analysis of the communication outage in Egypt by covering these two angles. First, I view the outage through an infrastructural lens. Working with a team of investigative journalists and activists, I collected primary evidence on how the cut actually took place, testing whether Egypt is a case of "new-school censorship", as posited by Jack Balkin[2] and explained in Chapter 1 of this book. Unlike traditional censorship means like physical force, detainment and court orders, Balkin defines new-school censorship as referring to the utilization of the information and telecommunications infrastructure and the use of third parties to censure and monitor the opposition and general public by the state. Second, I analyze the communication outage through an economic lens. I connect the dots to reveal a story of how technologically induced

economic shortages represent collateral damage, whereby economic liberty is curtailed by censorship. I study indicators of losses in the Information and Communications Technology (ICT) sector, providing conservative estimates that point to the overall losses.

By exploring these two aspects, I try to tap into the government censorship logic, which is manifested in the quest to control overall infrastructures, while disregarding the different implications, dubbed collateral, of this concentrated power. In this context, full control eventually becomes a key to more losses.

METHODOLOGY

This chapter has two major components. First, in order to uncover the story of how the outage took place, I conducted in depth interviews with individuals privy to this information. I also worked closely with several investigative reporters and activists striving to uncover the process by which the decision was made and implemented in late January 2011. The information and narratives collected are varied and at times conflicting owing to the secretive nature by which the outage was orchestrated. I offer the varying accounts, dubbed "Narrative 1" and "Narrative 2".

Second, in order to calculate the economic cost of the communication and Internet outage, detailed data from various sectors were required. In the absence of such data for Egypt, I relied on estimating the loss of the sectors that were most directly affected by the outage: mobile operators and Internet service providers (ISPs). These sectors point to economic losses and are not an aggregation of losses for the whole economy. As well, it is conceptually difficult to separate the marginal impact and economic costs of the SMS and Internet outage from the other costs of the disruptions caused by the revolution to whole sectors of the economy. I acknowledge this as a limitation of this work.

BACKGROUND: THE TECHNOLOGICAL INFRASTRUCTURE

To understand how the Internet was switched off in Egypt it is important to lay out how the telecommunication infrastructure is set up from a technological perspective, and also how it is shaped and centralized by legal constraints. The infrastructural setup of the telecommunication industry in Egypt already shows the tendency to centralize, which effectively

allows the state to maintain control over the most important parts of the telecommunication infrastructure. For instance, private ownership over telecommunication infrastructure was not allowed by the Egyptian state until 1998, but until today the state retains a monopoly over the infrastructure, predominantly owned by Telecom Egypt (TE). TE is the state-owned telecommunications company which in turn offers wholesale services to different licensed operators.

The telecommunications infrastructure in Egypt is built on the backbone of TE.[3] A core element of the infrastructure is a series of so called media gateways (MGW), collectively known as core networks (CNs) — which in Egypt are popularly referred to as the "centrals" in the local language.[4] Different CNs house equipment that process voice and data information and reroute it as needed; this includes equipment for landlines, 2G and 3G cellular technologies, as well as the Internet.[5] CNs bundle information from the so-called base switching centres (BSCs), or simply "switches". CNs also send this information to a supervision centre at each respective mobile and Internet service provider, named the network operations centres (NOCs). Each NOC manages and maintains the entire telecommunications system.[6] At the NOC, the mobile or Internet service provider can presumably shut down the connection in a specific area for maintenance purposes, e.g., to fix faulty equipment.[7]

Hossam Saleh, the president of the Internet Society of Egypt,[8] explained that there was a myriad of CNs stationed around the country, mainly located at the centre of major cities. These CNs have various floor levels that house the mobile and Internet equipment.[9] This equipment is housed in room-like structures and allows the entire system to work. All CNs are owned and operated by TE, which rents out space on its property for all the mobile and Internet service providers to house their equipment.[10] Three main CNs in Cairo are responsible for the operations of about 70 per cent of the entire Egyptian telecommunications grid.[11] These CNs are fed by alternative electricity and telecommunication connection sources to ensure system stability and avoid any blackouts.[12]

Egypt's Internet connection comes in through international bandwidth fibre-optic cables that connect Egypt via the local CNs.[13] In early 2011, there were nine[14] cables that come into Egypt through various CNs.[15] These cables, which are called "transmission rings", are connected to

devices owned by TE and its ISP, TE Data.[16] The Internet is then once more connected to other transmission rings owned by TE Data, which further connect these cables to the outside world.[17] Hence, all ISPs are connected to the international Internet cloud via Telecom Egypt.[18]

The Ministry for Communication and Information Technology (MCIT) and the National Telecommunication Regulation Authority (NTRA) retain their control over the telecom infrastructure. This is done via a system of different licences which grant the private sector access to this infrastructure. The private sector — composed of several privately owned companies such as Mobinil, Vodafone and Etisalat and other ISPs, as well as TE which is partially owned by the state — in turn offers its services to the population.

Telecom Egypt is a joint stock company over which the Egyptian government retains majority control (80%).[19] TE leases out wholesale services to a variety of ISPs, of which there were 220 different companies in Egypt in 2010, just before the communication cut in January 2011. There are three different classes of licences for ISPs in Egypt: Class A, Class B, and Class C licences. The Class A licence accords the right to own telecommunications infrastructure. The Class A licence also grants direct rights to access Telecom Egypt's international gateways through which Egypt is connected to the Internet. This allows Class A licensed ISPs to offer wholesale services to Class B and Class C ISPs, who in turn offer retail Internet services to the public. All fibre-optic cables are leased out by TE to the different ISPs.

The largest ISP in Egypt is TE Data, which is one of the four ISPs retaining Class A licence. The other three are LINKdotEGYPT (owned by Mobinil), Nile Online and Egynet (both owned by Etisalat). Holders of Class B licences include Raya (owned by Vodafone), YallaMisr, Noor, and Menanet.[20] TE Data offers its services to most of the governmental and security apparatuses of the state, including the Presidency.[21] It also owns 90 percent of the telecommunications infrastructure of Egypt. In this way, TE has a virtual monopoly over the telecommunication industry in Egypt.[22]

BACKGROUND: THE LEGAL INFRASTRUCTURE

Two laws enabled the regime to assume control over telecommunica-

tions in early 2011. The first was the 1981 Emergency Law, which remained in effect until the Supreme Council of the Armed Forces (SCAF) put an end to it on May 31, 2012. The Mubarak regime safeguarded its actions through Article 3 of the Emergency Law, which allowed the government to monitor, and censor the press, and all personal communication platforms.[23]

These broad-based powers were later bolstered by the enactment of the Telecommunication Law of 2003.[24] This law brought into existence NTRA. The NTRA's mandate was to regulate the telecommunication service and also to "protect [n]ational [s]ecurity, and the [s]tate['s] top interests",[25] as exemplified by Article 67. It reads,

> *The state competent authorities shall have the power to subject to their administration all telecommunication services and networks of any operator or service provider and call operation and maintenance employees of such services and networks in case of natural or environmental disasters or during declared periods of general mobilization in accordance with the provisions of Law No. 87 of 1960 or any other cases concerning National Security.*[26]

In addition, Article 68 absolves the ISPs from any legal censure that might occur from cooperating with state-given directions as well as ensures compensation for any damages that they may incur.[27] NTRA's board is composed of several high level officials from the Ministries of Defence and Finance, national security entities, as well as representatives of users and telecommunication experts.[28] Thus, the Telecommunication Law of 2003 shows the potential of using state authority as a means of censorship and surveillance. Egypt's technological and legal telecommunication infrastructure exemplifies the new-school censorship as defined by Balkin.

A HISTORY OF CONTROL

After January 2011, several State Security Investigation Service (the Internal intelligence agency, known as 'State Security' for short) documents were leaked. Some of these were made available to the public in the memorable break-in at State Security headquarters in Cairo less than a month after Mubarak's departure on March 8, 2011. The leaked documents show the high degree of monitoring and surveillance of the population, espe-

cially activists, carried out by the Mubarak regime.

For example, leaked documents suggest that the Mubarak regime had assembled an "emergency task force" after the clashes that erupted in the wake of the April 6, 2008 workers strike.[29] This task force was mandated to discuss and initiate new methods to censure and survey the Internet and all other forms of communication. The emergency task force was composed of high-level representatives from the State Security, Ministry of Interior and senior representatives of the mobile operators in Egypt.[30] In their discussion, outlined in the leaked meeting minutes, the task force deliberated and explored ways to block Internet services in certain cities, slow or shut down certain websites, identify Internet users' IDs for further investigation, and block the mobile services of the present three operators in cities as they saw fit.[31] Surprisingly, in October 2010, under the pretence of mobilization in case of the event of a security threat, this group executed a simulation communication cut-off.[32] This simulation included shutting off Internet and mobile services in villages and cities in a "timely fashion".[33] The simulations also included identifying Internet users using electronic fingerprints and blocking certain websites. The leaked meeting minutes revealed that these simulations faced some drawbacks, especially in regards to blocking websites.[34]

State Security forces did not only use the MCIT for censorship and surveillance, but they also relied on the ISPs themselves.[35] State Security forces did not contact the ISPs' managing directors or chairmen; instead they directly contacted individuals working in the technical departments.[36] Those individuals would receive calls from State Security personnel telling them to take down a website, check the activities of a certain individual they were watching, or see if anyone was sending bulk emails and less frequently check the content of messages.[37]

Checking message content was a less preferred option by State Security, as it would have meant hacking a user's account. This would result in a loss of the password, and would thus alert the user to the surveillance. This would in turn stop the user's online activity, and hence counteract the surveillance efforts.[38] Additionally, ISPs in Egypt operate under the legal scope set out by the law, which officially prevents them or State Security from infringing on personal freedoms.[39] Hence, for the most part, ISPs were "clean" in their dealings as institutions.[40]

The Ministry of Interior also had its own Internet and communication surveillance centre. Called the Department of Information and Documentation, this centre took part in the above-mentioned task force. Together, these departments maintained an ongoing watch on the general populace.[41]

Leaked documents from a meeting on January 1, 2011 included evidence that the Mubarak regime planned the purchase of elaborate surveillance systems. [42] As stated in the documents, during this meeting high-ranking State Security officials were reviewing surveillance software called FinFisher, which is developed by a British-German company that specializes in surveillance products called Gamma International. The software would allow the state to undertake surveillance through remote intrusion solutions, referred to as FinSpy, and remote infection tools, referred to as FinFly.[43] FinFisher was offered to the regime at 388,604 Euros. The government received a demo package to try out the software for five months.[44] FinSpy and FinFly would allow the government to monitor a target's e-mail, voice and video traffic (e.g., Skype calls), extract files and documents, log all key-presses, and enable live surveillance through the target's web-cam and microphone.[45] It is important to note that the leaked documents do not confirm the purchase of FinFisher prior or subsequent to the January 25 Revolution.[46]

This analysis does not show the full picture of censorship in Egypt. It does, however, include evidence that the state used both new-school and old-school censorship tactics to control political dissent. Due to both missing information and disjointed accounts, the full picture of the censorship infrastructure remains difficult to paint fully.

THE STORY BEHIND THE OUTAGE

Narrative 1

As I already mentioned, this section relies entirely on narratives from interviews with activists and local experts, some of whom chose to stay anonymous.[47] I, therefore, draw attention to the fact that there are two different narratives explaining the events leading up to the Egyptian Internet outage in January 2011. I will present each narrative below based on the information I gathered.

Narrative 1

The first account is given by two engineers who fathom that the communication outage occurred at the ISPs' centralized NOCs in the presence of a technician and "probably" a State Security officer.[48] There was no "kill-switch" as such, but rather, a software was used to simply disable, or "switch off", the functionality of the communication system.[49] This is supported by the argument that communication was not cut at one point in time across the nation but rather in a domino effect.

A third engineer interviewed separately confirmed this information. He discerned that the cutting-off of Blackberry Messenger (BBM) services and Short Messaging System (SMS) in the mobile operators happened through a ready-to-use program, whereby engineers injected a script into their customer database to shut down the systems.[50] The higher the number of subscribers to a particular service, the more time the script would take to run.[51] In this way, cutting services like the BBM service or any other data service would take less time than cutting-off a common service like SMS or mobile calls.[52] The technology engineer believes that it took the mobile operators Mobinil and Vodafone about three hours to fully shut down the BBM service.[53]

The blog of Renesys, an Internet monitoring authority, offered evidence to this effect by documenting the sequence of the shut-off of the Egyptian communication outage in January 2011. It stated that the communication outage was not an instantaneous event: each service provider appeared to have approached the task of shutting down its part of the Egyptian Internet separately upon government orders. [54] The Renesys blog states that on Thursday, January 27, 2011, the Egyptian Internet outage started at 22:00, when all Internet service providers were cut off, except for one — Noor.[55]

ISPs were mentioned on the blog in chronological order of being cut-off:

- Telecom Egypt[56] (AS8452), starts the process at 22:12:43;
- VF: Raya[57] joins in a minute later, at 22:13:26;
- MN: Link Egypt[58] (AS24863) begins taking themselves down 4 minutes later, at 22:17:10;
- Etisalat Misr[59] (AS32992), a mobile operator, goes two minutes

later, at 22:19:02;

- Internet Egypt[60] (AS5536) goes six minutes later, at 22:25:10.[61]
- As such, this narrative presents a story where the shutdown took place at the ISP level, implemented in accordance with government orders.

Narrative 2

Unlike the first narrative that accords a relatively active role by the ISPs, the second narrative presents a different situation where the cut-off was implemented at the government CNs. This narrative explains that the communication cut-off was fully implemented by the Ministry of Interior and the State Security, with authorization from the Presidency and the Prime Minister. The cut-off was facilitated by overwhelming state control and the centralized nature of the telecommunications infrastructure in Egypt, as discussed earlier. My anonymous sources, experts on the technical and legal situation regarding the Internet in Egypt, argued that the infrastructure could effortlessly be used for censorship and surveillance. They explained that the possibilities for censorship were part and parcel of the Internet infrastructure through legal provisions, the authority responsible over it as well as the tactics that State Security and the Ministry of Interior used. There was a plan in place should the need arise to shut down the system, but it required agreements and going through the correct legal channels. The leaked documents regarding the shut down simulation confirm this.

According to a source from the telecommunications industry, who preferred to remain anonymous, the communication outage story commenced with State Security personnel noticing, through their Department of Technological Information, that there was an increased hype on Facebook pages such as 'Kolena Khaled Said' ("We are all Khaled Said"), and other social media sites. These pages showed a lot of more "serious talk" about orchestrating a protest on January 25, 2011. Consequentially, State Security called a meeting with the Ministry of Interior's cybercrime unit ten days before the planned protest (this would have been January 15, 2011). At another meeting with the Morale Affairs Department of the Armed Forces, security officials discussed whether these events would be considered a serious threat against the regime that required action. Even

though State Security regarded the unfolding events as alarming, the meeting did not end with a decision being taken. Similarly, it seemed that the Presidency saw no need for immediate action.[62]

On January 20, 2011, there was a small protest in Tahrir Square in order to gauge the level of support activists might receive on January 25. Around 500 protesters showed up. Encouraged, they decided to go ahead with the larger protest planned for January 25. On January 24, the Presidency is said to have contacted State Security and told them to take the "necessary precautions," which meant reverting to the old-school censorship means of rounding up and arresting activists. This tactic was not only used to put prominent activists out of action by detaining them for a few days until the hype died down, but also to frighten the opposition by reminding them that they were under surveillance.[63]

The January 25 protest turnout was larger than expected. The momentum of the protest continued with a stamina hitherto unseen on January 26, while the intensity extended outside of Cairo, especially in Alexandria and Suez. Protest organizers decided that January 27 would be a rest day and that on Friday, January 28, they would again turn up in full force.[64]

At this point, the Presidency is said to have informed State Security to use whatever necessary means needed to regain control. To do this, State Security is said to have called a meeting with all responsible ministries and individuals on the morning of January 27, where they articulated that they needed to gain control of all telecommunication networks in Egypt. Although there were concerns raised by other ministerial heads, who stated that they would need to do this through proper legal channels, State Security replied that there was no time to do so. These actions, they stipulated, would have had to be taken with the consent of the President. At that point, State Security is said to have stated, they were not able to keep up with the amount of chatter on Facebook and Twitter, and that there was no way to salvage the situation. They relayed this information to the Minister of Interior, who asked for a contingency plan.[65]

When State Security reached out to the president of NTRA, he replied that he would not let them use his institution to illegally cut communications, but he offered to gather the heads of the ISPs and mobile operators in a meeting to deliberate what can be done. The meeting was set for 16:00

on January 27, in Smart Village, Cairo's technology hub. Those present in the meeting were the heads of TE Data, TE, Vodafone, Mobinil and Etisalat, State Security representatives and the governors of Cairo, 6th of October City, and Giza, along with the Minister of Interior via conference call. In this meeting, State Security explained that they would take over the telecommunications network since it was, and continues to be, a strategic tool of the opposition, because the situation was unsalvageable. ISPs are said to have informed State Security that they could shut down the entire system by simply disabling the "switches" located at key CNs around the country. Inside each CN there were "test rooms" that house these switches for all mobile and ISPs. They stated that they would give the keys of their respective switches to State Security at 08:00 the next day. State Security could then send their officers to the CNs and turn off all connections. These switches had never been turned off since the commencement of telecommunications in Egypt over 60 years ago. This, however, was not how the cut happened.[66]

On the evening of January 27, State Security started taking action to contain the communication between activists. At first they told ISPs to shut down Blackberry services, and then other data applications such as Facebook on mobiles, followed by Twitter.[67] This is corroborated by the first narrative based on the accounts of three engineers interviewed separately.

According to this second narrative, this activity was noticed quickly by the activist community. Rather than deterring the bustle, activists started to reroute traffic using multiple proxies. This made it more difficult for State Security to track the activity and block it. More so, activists started spreading the word that if all communication were to be cut then there was a standing time and place to meet. The overall Internet activity did, of course, decrease.[68]

By 21:00 that evening, State Security is said to have told all ISPs and mobile service providers to be "on call" on their premises. This was highly suspicious to all telecommunication workers in each of the companies, as it was a Thursday night (the start of the weekend in Egypt) and the management would not give them detailed reasons as to their late stay. The general consensus between workers was that there was going to be a major telecommunications shut down, which they suspected would occur on Fri-

day afternoon. This information started to leak out to activists. [69]

Those responsible at this point in time were State Security and Ministry of Interior personnel. These individuals were trained old-school soldiers and did not fully comprehend the ease or speed by which information could move or be used by the tech-savvy youth activists. Around 01:00 on Friday, January 28, State Security began to receive information that activists were exchanging landline numbers in anticipation of a cut in all forms of communication cut off. As a result, State Security officials panicked and decided not to wait to receive the allotted keys at 08:00 the next day, but to forcibly break into the CNs. Thus, January 28 became the day that the communication outage took place for both the Internet and mobile telephones.[70]

After shutting down the Internet, State Security called the ISPs and told them to send their personnel home. Unable to get in contact with anyone from the Ministry of Communications and Information Technology, ISPs are said to have complied. However, they sent several of their personnel over to the CNs the next day in order to try to turn the system back on, only to find that they were being guarded by the police who threatened to shoot anyone who approached them. In fact, State Security did not relinquish their hold on the CNs until February 12. By that time State Security had been driven out and they were too concerned with covering up any incriminating information to call off this particular security measure.[71]

As there was no official plan of action for the communication outage, State Security failed to switch off one of the ISPs, Noor. Noor was not called to the original meeting between State Security and ISPs, hence they did not provide them with their connection switches. Coincidentally, one of Noor's connection points happened to be on a transmission ring used only by TE Data. TE Data had left this switch off the list, so it would be able to reroute it to the Presidency or State Security should the need arise. Once the cut-off occurred, Noor realized that it had this working link. In order to divert attention from their link, Noor is said to have turned it off and on — probably from their NOC. Also since State Security had dispersed, there was no one to notice its existence, or act to stop Noor.[72]

According to our sources for this narrative, it was State Security rather than ISP personnel that played a proactive role in the communication out-

age. Using the switch map that they were provided by the ISPs and mobile operators at the meeting earlier, State Security shut down all power sources to these switches, and especially to the transmission rings that fed all ISPs. Therefore, this narrative is one where the Egyptian kill-switch was not a telecommunications cut of any sort but rather a power switch-off, meaning State Security did not damage the Internet infrastructure in any way. The international bandwidth cables were still operational, however there was no Internet traffic coming from Egypt for the cables to transport.[73]

NEW-SCHOOL OR OLD-SCHOOL CENSORSHIP?

There are two narratives to Egypt's communication cut-off. The first narrative highlights a more active role played by the private sector with pressure from the government. Different private sector entities were involved, as evidenced by the switching off of Blackberry messaging, 3G, landline Internet access at different times in different regions.[74] This public-private cooperation is part of what Balkin calls new-school censorship. As the background of control shows, evidence points to new-school censorship increasingly being used in Egypt before the 2011 cut.[75]

The second narrative emphasizes a stronger role played by State Security in actively shutting down the Internet access, with the acquiescence of the ISPs. This narrative included a higher degree of intimidation of the ISPs by State Security, leaning towards old-school censorship, albeit using new technologies. Indeed, old-school censorship had never left Egypt. The case of Egypt, one may argue, presented elements of both old and new censorship. In both stories, the communications cut came in accordance with the law.

COLLATERAL DAMAGE?

The private sector played a role in the communication cut-off. The actual role and its extent varied depending on the narrative. Ironically, these very ISPs and mobile operators did pay a price for this role. Their economic losses came within a larger damage inflicted on the whole economy.

It is important to highlight that Egypt's ICT sector was hailed as the flagship of the country's economic success in the 2000s. Mubarak's economic liberalization policies entailed investing heavily in infrastructure,

particularly telecommunications, which led media privatization in line with the development of Egypt's data backbone. ICT revenues grew steadily since 2005. In 2010, Egypt's ICT exports revenues amounted to US$ 1.1 billion, with the goal of reaching US$ 5–6 billion by 2020.[76]

When the government shut down the Internet and mobile communication channels, it meant to constrain political expression. Paradoxically, this action mobilized citizens to protest on the street and retroactively curtailed economic activity, stifling the economic growth the regime was promoting. In the quarter preceding the uprising, Egypt's economy was growing at 5.7 percent.[77] By March 2011, Egypt had an ousted president and a negative economic growth rate of -3.8 per cent.[78] In this way the regime essentially shot itself in the foot. The government-imposed communication outage is a manifestation of this asymmetry between political and economic freedoms.

In this section, I look into the economic impact of the communication outage on selected sectors of the economy, which mostly rely on Internet and communication, namely mobile and ISP sectors. Numerous sectors of the Egyptian economy operationally rely on the Internet, which makes isolating and calculating such losses challenging. This is amplified by the difficulty of separating the economic impact of the communication outage from the implications of political unrest in general.

There are two viable approaches to assessing the economic impact of the communication outage. The first is to estimate the loss to the ICT sector as a whole from a macro perspective. The second is a micro approach of calculating the loss of specific sectors. In all cases, these approaches provide indications of the losses and not an aggregation of them. In this study, I attempt to estimate the economic losses, once through a macro approach, then move on to calculate losses of specific ICT sectors namely mobile operators and ISPs as examples.

LOSSES TO THE ICT SECTOR

An Organization for Economic Cooperation and Development (OECD) study used the macro approach, estimating that each day the outage produced an economic loss of US$ 18 million to the Egyptian economy, totalling a minimum of US$ 90 million in losses during the five days of outage.[79] Forbes estimated a higher amount of loss, US$ 110 million,

after adding lost outsourcing revenues from call centres (US$ 3 million per day) and an additional US$ 1 million per day for ICT-dependent industries.[80] A third estimate was provided by Curt Hopkins, who viewed the Forbes figure as conservative, and estimated the total loss at US$ 135 million.[81]

To estimate losses of the ICT sector, I multiplied the daily revenue of the sector by five days of outage, taking the daily revenue of 2010 as proxy for the daily revenue in 2011.[82] The total annual revenue of the sector was US$ 7.8 billion,[83] which meant an average daily revenue of US$ 21.3 million. Losses for the five days therefore are estimated at US$ 106.7 million.

An Egyptian administrative court ruling in 2011 fined Mubarak, his Prime Minister, and his Minister of Interior an amount of EGP 540 million (US$ 91 million) for cutting mobile and Internet services.[84] The lawsuit was raised by human rights organizations against them for cutting mobile, Internet services and thus hampering citizens' freedoms.

Table 1: Summary of ICT losses (macro approach) (figures in US$ million)

Sector	Revenue in 2010	Daily losses	Number of days sector affected	Total losses
Macro Approach				
ICT	7800	21.3	5	106.5

Source: Extrapolation from Ministry of Communications and Information Technology, ICT Indicators Bulletin, 2010.

LOSSES TO SPECIFIC SECTORS: A MICRO APPROACH

Internet Service Providers

The Egyptian ISP market is open to the private sector and amounted to 220 companies in 2010.[85] Due to the dearth of data on ISPs in Egypt, we could only find revenues for 2008. We projected the revenues for 2010 by using the increase in the number of Internet users over the two years, estimating ISPs revenues for 2010 at US$ 1.1 billion.[86] Daily revenues therefore stood at US$ 2.97 million. Over the five-day period, the estimated

losses were approximately US$ 14.85 million. Table 2 illustrates these figures.

Table 2: Summary of ISP losses (micro approach) (figures in US$ million)

Sector	Revenue in 2010	Daily losses	Number of days affected	Total losses
Micro Approach				
ISPs	1100	3.01	5	15

Source: MCIT revenue figures for 2008, users number from 2010.

Mobile Operators

While text messaging was cut for eight days, mobile calls were blocked for one day. I used all the available data to separate revenues of text messaging (SMS) from mobile calling (voice). Based on one day blocking of voice service, I have estimated the minimum loss to be between US$ 8.9 and US$ 9.6 million. Based on eight days of blocking of SMS services, I estimate the minimum loss to be US$ 6.3 million. This makes the total estimated loss of mobile operators between US$ 15–16 million.

This figure coincides with the estimated compensation to mobile operator pledged by MCIT in 2011.[87] This amount equalled LE100 million, which is equivalent to US$ 16.4 million. Table 3 below illustrates the figures above.

My estimates are conservative and point to a minimal loss rather than a comprehensive account of damages. I point to daily losses for the ICT sector as a whole (macro approach) amounting to US$ 21 million, adding up to US$ 107 million. From the micro approach, I point to minimal daily losses in the two selected sectors of US$ 13.5 million,[88] with a total of about US$ 31 million (US$ 15 million in ISP sector, and US$ 16 million in the mobile sector).

Table 3: Estimated daily revenues of mobile operators (in US$ 100,000)

Based on Q1 2011 revenues/90 days	Mobinil	Vodafone	Etislat Misr	Total
Micro Approach				
Daily Revenues (Data)	3.67	6.3	1.6	10
Daily Revenues (SMS)	370	310	110	790
SMS Revenues (8 days)	2940	2490	880	6310
Daily Revenues (Voice)	4120	3860	1690	9670
Total loss estimated	7060	6350	2570	**15990**

Source: Calculated based on data set from Informa Telecom & Media Ltd., UK. (Most conservative estimate as mobile calls were blocked for 1 day while SMS were blocked for 8 days.)

CONCLUSION

In this chapter I have tried to examine two under-studied issues related to Egypt's communication outage of January–February 2011. First, I have tried to show the story behind the actual outage, illustrating it to be a combination of both old-school and new-school censorship that were prevalent during Mubarak's dictatorial regime. Old-school censorship recurs, building over the scale of the new-school censorship architecture constructed by the regime and propagated in order to place a communication and information embargo to bolster classic censorship tactics.

Second, I have pointed to the detrimental effects on the classical economic liberties that occur when censorship, particularly in its infrastructural form, is utilized by the state. Part of that damage happens to those very agents that collaborated with the State. In this manner, economic liberty becomes forgotten in lieu of the political interests of the ruling regime. I have tried to unpack the economic impact acknowledging that economic liberties and expressive liberties are not disconnected. Indeed, I

have emphasized that we should not treat political and economic impact as a binary or as two distinct implications. I have argued for the importance of studying politics and economics in tandem in Egypt and beyond, and for analytical work that connects individual expressive and economic liberties.

Whether new-school or old-school censorship, cutting Egypt's communication with the rest of the world had serious political and economic implications. Additionally, with a communication outage that cuts people off from ambulances, medics, family and friends, the immeasurable collateral damage was in the lives lost and the wounded victims of shootings who were left unrescued thanks to Mubarak's communication outage.

1 The author is thankful to the interviewees, some of whom preferred to stay anonymous. Gratitude also goes to Hossam Saleh for his insights and for his help in reviewing and fact-checking the chapter. The author is indebted to Lina Attalah for her contribution to, and review of, the research. The author also acknowledges the research assistance of May Khourshed and Shereen Nasef. Stefanie Felsberger and Nagham El Houssamy contributed to reviewing this work.

2 These concepts were outlined by Jack Balkin in his speech at the Global Censorship conference organized by the Information Society Project at Yale Law School in March 2010, and later published in an article. See generally Jack Balkin, *Old-School/New-School Speech Regulation*, 127 HARV. L. REV. 2296 (2014), available at http://cdn.harvardlawreview.org/wp-content/uploads/2014/06/vol127_balkin.pdf.

3 Interview by Nagla Rizk, Farida Ezzat & May Khourshed with Hossam Saleh, President, Internet Society of Egypt, in Cairo (Mar. 31, 2013) [hereinafter Hossam Saleh].

4 *Id.*

5 Interview with Alcatal engineer (November 22, 2012), Cairo.

6 Hossam Saleh, *supra* note 85; Alcatal engineer, *supra* note 83.

7 Alcatal engineer, *supra* note 83.

8 Internet Society (ISOC) is a global organization with the aim of keeping the Internet free and open. The Egyptian Internet Society is the local chapter of this global institution. See Internet Society, ISOC Egypt Chapter Chartered (Mar. 1997), http://www.internetsociety.org/history-timeline/isoc-egypt-chapter-chartered.

9 Hossam Saleh, *supra* note 85; Alcatal engineer, *supra* note 83.

10 Hossam Saleh, *supra* note 85; Alcatal engineer, *supra* note 83.

11 Hossam Saleh, *supra* note 85.

12 *Id.*

13 Alcatal Communications engineer, *supra* note 83.

14 Today this number has risen to 14, according to Hossam Saleh. See Statement by Hossam Saleh, September 30, 2014.

15 Hossam Saleh, *supra* note 85.

16 *Id.*

17 Alcatal Communications Engineer, *supra* note 83.

18 Hossam Saleh, *supra* note 85.

19 Telecom Egypt, Company Fact Sheet, http://ir.te.eg/CompanyFactSheet.

20 This paragraph is based my research undertaken for the upcoming chapter Nagla Rizk, Media Concentration in Egypt, *in* INTERNATIONAL MEDIA OWNERSHIP AND CONCENTRATION (Eli Noam et al. eds., 2015).

21 Hossam Saleh, *supra* note 85.

22 *Id.*

23 The Emergency Law in Egypt, Int'l Federation of Human Rts. (Feb. 3, 2011), http://www.fidh.org/THE-EMERGENCY-LAW-IN-EGYPT.

24 Law No. 10 of 2003 (Telecommunication Regulation Law), National Telecommunication Regulation Authority (Feb. 4, 2003), available at http://www.tra.gov.eg/uploads/law/law_en.pdf.

25 *Id.*, art. 13(7).

26 *Id.*, art. 67.

27 *Id.*, art. 68.

28 *Id.*, art. 12.

29 Memorandum Regarding Bulk SMS Blocking (Sept. 30, 2010), Cairo; Memorandum on Censoring Bulk SMSes (Oct. 13, 2010); Emergency Task Force Minutes, October 2010.

30 Emergency Task Force Minutes, *supra* note 59.

31 Memorandum to Emergency Task Force on Blocking and Censuring the Internet and SMSes (Oct. 6, 2010); Censoring Bulk SMSes, *supra* note 59; Emergency Task Force Minutes, *supra* note 59.

32 Emergency Task Force Minutes, *supra* note 59.

33 *Id.*

34 *Id.*

35 Based on information collected from the following sources: Interview by Nagla Rizk, Farida Ezzat & May Khourshed with an anonymous communications engineer (Mar. 2013) [hereinafter Anonymous 1]; Interview by Nagla Rizk, Farida Ezzat, Nagham El Houssamy & Shereen Nassif with Ramy Raouf, Sarah Carr & Lina Attalah, in Cairo (Oct. 7, 2012) [hereinafter Raouf, Carr & Attalah]; Memo Regarding Bulk SMS Blocking, *supra* note 59; Emergency Task Force Minutes, *supra* note 59.

36 Emergency Task Force Minutes, *supra* note 59.

37 Anonymous 1, *supra* note 53.

38 *Id.*

39 Hossam Saleh, *supra* note 85.

40 *Id.*

41 Anonymous 1, *supra* note 53.

42 FinFisher File, Retrieved during March 8th 2011 Raid of State Security Headquarters (Jan. 1, 2011); Memorandum Regarding Capabilities of FinFisher (Dec. 22, 2010); Memorandum Regarding Possibly Looking into FinFisher Product (Aug. 15, 2009).

43 FinFisher File, *supra* note 46; Memo Regarding Capabilities of FinFisher, *supra* note 46.

44 FinFisher Proposal: Commercial Offer (June 29, 2010).

45 FinFisher File, *supra* note 46.

46 *Id.*

47 The chapter was sent to the interviewees for fact verification.

48 Interview by Ramy Raouf with a Mobinil engineer who preferred to stay anonymous, in Cairo (2011) [hereinafter 'Mobinil engineer']; Interview by Sarah Carr with anonymous communications engineer, in Cairo (2011) [hereinafter Anonymous 2].

49 Interview by Nagla Rizk with Ramy Raouf, September 25, 2014 [hereinafter 'Ramy Raouf'].

50 Raouf, Carr, & Attalah, *supra* note 53; Anonymous 2, *supra* note 40; Mobinil engineer, *supra* note 40.

51 Raouf, Carr, & Attalah, *supra* note 53; Anonymous 2, *supra* note 40.

52 Raouf, Carr, & Attalah, *supra* note 53; Anonymous 2, *supra* note 40.

53 Anonymous 2, *supra* note 40.

54 Jim Cowie, Egypt Leaves the Internet, Renesys Blog (Jan. 28, 2011), http://www.renesys.com/blog/2011/01/egypt-leaves-the-internet.shtml.

55 *Id.*

56 Here Renesys lists Telecom Egypt which is the owner of TE Data, the actual ISP. See Nagla Rizk, *supra* note 68.

57 Raya is an ISP owned by Vodafone. See Nagla Rizk, *supra* note 68.

58 Link Egypt was a company which provided turnkey Internet services and solutions in Egypt until 2000. In 2000, Link Egypt merged with InTouch Communications to become LINKdot-NEt, an Internet service provider owned by Mobinil. See LINKdotNET, Our History, http://www.link.net/English/Linkcorp/About/Our%20History/, LINKdotNET Homepage (last visited October 2014).

59 Etisalat Masr is a mobile operator who owns the ISP named Nile Online, to which Renesys was referring here.See Nagla Rizk, *supra* note 68.

60 Internet Egypt is a company which recently consolidated with EgyNet, a large ISP also owned by Etisalat. See Internet Egypt, Internet Egypt Infrastructure, http://internetegypt.com/Infrastructure.htm, Internet Egypt Homepage (last visited October 2014).

61 Cowie, *supra* note 34.

62 Anonymous 1, *supra* note 53.

63 *Id.*

64 *Id.*

65 *Id.*

66 *Id.*

67 *Id.*

68 *Id.*

69 *Id.*

70 *Id.*

71 *Id.*

72 *Id.*

73 *Id.*

74 Ramy Raouf, *supra* note 39.

75 Anonymous 1, *supra* note 53; see also FinFisher File, *supra* note 46; FinFisher Proposal: Commercial Offer, *supra* note 44; Memo Regarding Possibly Looking into FinFisher Product, *supra* note 46; Memorandum to Emergency Task Force on Blocking and Censuring the Internet and SMSes, *supra* note 57; Memo Regarding Capabilities of FinFisher, *supra* note 46; Censoring Bulk SMSes, *supra* note 59; and Memo Regarding Bulk SMS Blocking, *supra* note 59.

76 Destination Egypt: ITO-BPO Value Proposition, Info. Tech. Indus. Dev. Agency (Jan. 2012), http://www.itida.gov.eg/Documents/Combined%20ITO-BPO%20Value%20Prop%20January%202012%20-%20Analysts%20Visit.pdf.

77 Ministry of Finance, The Financial Monthly, MOF Publications, http://www.mof.gov.eg/English/publications/MOF_Publications/Pages/The_Financial_Monthly_Bulletin.aspx.

78 *Id.*

79 The Economic Impact of Shutting Down Internet and Mobile Phone Services in Egypt, Org.

for Econ. Cooperation & Dev. (Feb. 4, 2011), http://www.oecd.org/countries/egypt/theeconomicimpactofshuttingdowninternetandmobilephoneservicesinegypt.htm

80 Parmy Olsen, Egypt's Internet Blackout Cost More than OECD Estimates, Forbes (Mar. 2, 2011), http://www.forbes.com/sites/parmyolson/2011/02/03/how-much-did-five-days-of-no-internet-cost-egypt/.

81 Curt Hopkins, The Cost of Egypt's Internet Blackout: $110 Million+, ReadWrite (Feb. 6, 2011), http://readwrite.com/2011/02/06/the_cost_of_egypts_internet_blackout_110_million.

82 Quarterly ICT Report, Ministry of Comm. & Info. Tech. (Mar. 2012), http://www.mcit.gov.eg/Upcont/Documents/Publications_15102012000_ICT%20Indicator%20Eng-%20Mar%202012-5.pdf

83 ICT Bulletin – June 2012, Ministry of Comm. & Info. Tech. (Jun. 2012), http://www.egyptictindicators.gov.eg/en/Publications/PublicationsDoc/ICT%20Bulletin-%20June%202012.pdf.

84 Shaimaa Fayed, Egypt's Mubarak Fined for Communications Cut, Reuters (May 28, 2011), http://www.reuters.com/article/2011/05/28/us-court-egypt-idUSTRE74R0TA20110528.

85 Annual Report 2010: Egyptian Company for Mobile Services, Mobinil (2010), https://www.mobinil.com/en/about/investors/documents/2010annual_report.pdf.

86 ICT Bulletin – June 2012, *supra* note 5.

87 EgyNews (May 28, 2011), http://www.egynews.net/wps/portal/news?params=126156.

88 This figure is a total of ISP losses of US$ 5 million, SMS losses of US$ 0.8 million, and voice calling losses of US$ 9.6 million.

CONTRIBUTORS

ERIN BIEL

Erin Biel is the Director of Programs, Yangon at Partnership for Change, Myanmar. Erin has worked with the Yale Law School's Iraqi Refugee Assistance Project (IRAP), both in New Haven and while studying abroad in Cairo, providing legal representation and policy advocacy on behalf of Iraqi refugees seeking resettlement to the United States. Erin has also worked with the U.S. State Department's Bureau of Population, Refugees, and Migration, specifically focusing on individuals persecuted due to their sexual orientation.

Biel graduated from Yale University and received her B.A. in Global Affairs (International Security Track) and Ethnicity, Race, & Migration Double Major, Magna Cum Laude.

ALEXANDRE PACHECO DA SILVA

Alexandre Pacheco da Silva is a Ph.D. candidate in Science and Technology Policy at Campinas State University (Unicamp), and a senior researcher at Innovation Research Group (IRG), Getulio Vargas Foundation. He holds a LL.M. in Law and Development at Getulio Vargas Foundation.

ANJALI DALAL

Anjali Dalal is a 2L at the Yale Law School. In addition to being involved in the Information Society Project, Dalal is the Press Secretary for the national organization of Universities Allied for Essential Medicines (UAEM), and is actively involved with the Yale chapter as well. At the law

school, Anjali serves as submissions editor for the Yale Journal of Law and Technology, participates in the Workers and Immigrants Rights and Advocacy Clinic, and is the co-chair of the Immigration Issue Group within the American Constitution Society. Dalal interned with Google in Washington, D.C., working on policy and legal issues ranging from broadband access to privacy. She continues to work for Google in a part-time capacity.

Dalal is a native of Reading, Pennsylvania, in the United States of America. She graduated m*agna cum laude* from the University of Pennsylvania with a dual degree in Philosophy from the College of Arts and Sciences and Economics from the Wharton School.

LAURA DENARDIS

Laura DeNardis is a Research Scholar, Lecturer, and the Executive Director of the Information Society Project at Yale Law School. Prof. DeNardis is an Internet governance scholar and the author of Protocol Politics: The Globalization of Internet Governance (MIT Press: 2009), Information Technology in Theory (Thompson: 2007 with Pelin Aksoy), and numerous book chapters and articles.

DeNardis received a Ph.D. in Science and Technology Studies (STS) from Virginia Tech, a Master of Engineering degree from Cornell University, and a Bachelor of Arts degree in Engineering Science from Dartmouth College.

EVE GRAY

Eve Gray, who has a background in academic publishing, is working on a number of projects related to open access and scholarly communications at UCT, in South Africa and other African countries, funded by the Shuttleworth Foundation, the IDRC and the Open Society Institute. She is the Project Director of the Opening Scholarship Project. This project was established in June 2007 and is hosted by the Centre for Educational Technology (CET) at the UCT, and its main aim is to explore the opportunities that ICTs and open dissemination models could offer for enhanced communication and more effective knowledge dissemination in one South African university, namely UCT.

MARGOT KAMINSKI

Margot E. Kaminski was a Research Scholar in Law, Executive Director of the Information Society Project, and Lecturer in Law at Yale Law School. She is a graduate of Harvard University and Yale Law School and a former fellow of the Information Society Project. While at Yale Law School, she was a Knight Law and Media Scholar and co-founder of the Media Freedom and Information Access Practicum. Following graduation from Yale Law School, she clerked for the Honourable Andrew J. Kleinfeld of the Ninth Circuit Court of Appeals. She has been a Radcliffe Research Fellow at Harvard and a Google Policy Fellow at the Electronic Frontier Foundation. Her research and advocacy work focuses on media freedom, online civil liberties, data mining, and surveillance issues. She has written widely on law and technology issues for law journals and the popular press, and has drawn public attention to the civil liberties issues surrounding the Anti-Counterfeiting Trade Agreement.

CHRISTINA MULLIGAN

Christina M. Mulligan is a Postdoctoral Associate in Law and Kauffman Fellow of the Information Society Project at Yale Law School. She previously served as a law clerk in the chambers of Judge Charles F. Lettow at the United States Court of Federal Claims, a visiting fellow of the Information Society Project, and a staff attorney at the Institute for Justice.

She holds B.A. and J.D. degrees from Harvard.

CAROLINE NCUBE

Caroline Ncube holds a PhD from the University of Cape Town. Her doctoral thesis examined the intellectual property protection of e-commerce business methods within the context of South Africa's tourism SMEs. She obtained her LLB from the University of Zimbabwe and her LLM from the University of Cambridge where she majored in Intellectual Property Law and Company Law. Caroline joined the Department of Commercial Law in 2005 and before that she lectured at the University of Limpopo (formerly University of the North) and the University of Zimbabwe.

Caroline plays an active role in various professional associations and participates in socially responsive research projects. She is often invited to give lectures and seminars on Intellectual Property to various constituencies, including WIPO Summer School students and librarians. Caroline is also actively involved in research projects that focus on open development, access to knowledge and the promotion of a balanced approach to IP.

PRANESH PRAKASH

Pranesh Prakash is a Policy Director at — and was part of the founding team of — the Centre for Internet and Society, a Bangalore-based non-profit that engages in research and policy advocacy. He is also the Legal Lead at Creative Commons India, and was an Access to Knowledge Fellow at the Yale Law School's Information Society Project. In 2014 he was selected by Forbes India for its inaugural "30 under 30" list of young achievers, and in 2012 he was nominated as an Internet Freedom Fellow by the U.S. government.

His research interests converge at the intersections of technology, culture, economics and the law. His current work focusses on interrogating, promoting, and engaging with policymakers on the areas of access to knowledge (primarily copyright reform), 'openness' (including open government data, open standards, free/libre/open source software, and open access), freedom of expression, privacy and Internet governance. He is a prominent voice on these issues, with the newspaper Mint calling him "one of the clearest thinkers in this area", and his research has been quoted in Indian parliamentary debates, as also in the New York Times, the Hindu, Washington Post, and numerous other publications.

He has a degree in arts and law from the National Law School in Bangalore, and while there he helped found the Indian Journal of Law and Technology, and was part of its editorial board for two years.

ANDREW RENS

Andrew Rens is a scholar of the complex interactions of law, knowledge, and innovation.

Rens teaches in Access to Medicines: Intellectual Property and Global Public Health at Duke Law. He is a Research Associate at the Center for

the Study of the Public Domain, and is writing a dissertation on the use of open licences in education at Duke Law School where he is an SJD candidate. Rens taught courses in Intellectual Property, Telecommunications, Broadcasting, Space and Satellite, and Media and Information Technology Law in the Law School at the University of the Witwatersrand, before spending several years in San Francisco, California, where he was a fellow at the Stanford Center for Internet and Society. He was the founding Legal Lead of Creative Commons South Africa and co-founder and former director of two nonprofit organizations: The African Commons Project, and Freedom to Innovate South Africa.

Rens was awarded the degrees of Bachelor of Arts, Bachelor of Laws (JD equivalent degree), and Master of Laws at the University of the Witwatersrand, Johannesburg.

NAGLA RIZK

Nagla Rizk is Professor of Economics and Founding Director of the Access to Knowledge for Development Center (A2K4D) at the School of Business at the American University in Cairo. Rizk is Faculty Associate at the Berkman Center for Internet and Society at Harvard University and an affiliated fellow of the Information Society Project at Yale Law School. Her area of research is the economics of knowledge, information technology, and development, with focus on business models in the digital economy, intellectual property, and human development.

She is also member of the advisory board of the IQsensato international research and policy think tank and of the board of the Genero Initiative for copyright.

Rizk is member of the Executive Committee of the International Economic Association, a founding member of the Access to Knowledge Global Academy and member of the steering committee of the Open Africa Innovation Research Project (Open A.I.R.). She wrote the National Strategy for Free and Open Source Software in Egypt. She received her Ph.D. in economics from McMaster University in Canada, and her M.A. and B.A. in economics from AUC.

MÔNICA STEFFEN GUISE ROSINA

Monica Steffen Guise Rosina is a Professor at Fundação Getulio Vargas Law School in São Paulo, where she coordinates the Research Group on Law and Innovation and teaches Intellectual Property, Legal Research, Fashion Law, and Digital Democracy. She holds a Ph.D. in International and Comparative Law from the University of São Paulo (2011) and an LL.M. from the Federal University of Santa Catarina (2006).

CARLOS AFFONSO SOUZA

Carlos Affonso Souza is a founder and director of the Institute for Technology and Society in Rio de Janeiro (ITS). He is an Affiliated Fellow at Yale Law School's Information Society Project and a Policy Fellow at Access. Dr. Souza was the vice-Director and co-founder of the Center for Technology and Society at Getulio Vargas Foundation. He teaches graduate and post-graduate courses at the State University of Rio de Janeiro (UERJ) and at the Catholic University (PUC-Rio) on intellectual property and internet governance and regulation. He has been a member of the Copyright Commission of the Brazilian Bar Association (Rio de Janeiro section) since 2007 and was a member of the former Commission for the Protection of Consumers in E-commerce, created by the Brazilian Ministry of Justice (2006-2008). Dr. Souza has been involved in many Internet governance activities at ICANN and at the United Nation's Internet Governance Forum (IGF). He holds a Doctoral and a Master degree in Civil Law from the University of the State of Rio de Janeiro (UERJ, 2009 and 2003) and a J.D. from the Catholic University of Rio de Janeiro (PUC-Rio, 2000).

REBECCA WEXLER

Rebecca Wexler is a student fellow of the Information Society Project at Yale Law School, where she is a J.D. candidate. She earned an M.Phil. in History and Philosophy of Science and Technology from Cambridge University (high first distinction), where she studied as a Gates-Cambridge Scholar; and a B.A. in History of Science and Women's Studies from Harvard College (*summa cum laude*).

After that, she spent seven years working as a documentary filmmaker making movies for television, art galleries, and theaters, during which time

she co-founded and served as instructor for the Yale Visual Law Project teaching visual advocacy to law students. She recently returned from studying post-war media production as a Fulbright Senior Research Scholar in Sri Lanka, where she taught documentary methods, history, and theory at the Eastern University of Sri Lanka, Trincomalee Campus.

HONG XUE

Hong Xue is a Professor of Law and the Director of the Institute for the Internet Policy & Law at Beijing Normal University.

Prof. Xue was elected as a 'Top Ten Nationally Distinguished Young Jurists' by the China Law Society. She is a Fellow of Yale Information Society Project and the Chinese Representative to Global Academy on Access to Knowledge. She has taught at Yale Law School, the Law Faculty of University of Hong Kong, the Law School of Murdoch University in Australia, and the World Intellectual Property Academy. She is invited to teach as professor at Torino Law School-WIPO Master of Laws in Intellectual Property and the Faculty Chair of Asia Pacific Internet Leadership Project (APILP). She is appointed by the United Nations Economic and Social Commission for Asia and the Pacific (ESCAP) to the United Nations Network of Experts for Paperless Trade in Asia and the Pacific (UNNExT). She has served as a founding member and IDN Liaison of the ICANN At-Large Advisory Committee (ALAC) and was appointed on the ICANN President's Advisory Committee on Internationalized Domain Names. She was the Chair of Asia Pacific Regional At-Large Organization (APRALO). She is a founding member of Chinese Domain Names Consortium (CDNC).

ACCESS TO KNOWLEDGE RESEARCH SERIES

GLOBAL CENSORSHIP

Shifting Modes, Persisting Paradigms

Freedom of expression depends not only on the mere absence of restrictions, but also on infrastructures of free expression, which are open and accessible. Taking that idea as its starting point, this book traces the metamorphosis of the methods and modes used by states—and private corporations—to shape and to control speech, hastened, as it has been, by the emergence of digital publics.

In a series of ten case studies covering eight countries—China, Myanmar, Sri Lanka, India, Egypt, Zimbabwe, South Africa, Brazil, and the United States of America—and two essays that provide an overall theoretical framework for these changes, this book reveals some of the changes we are seeing in the nature of censorship itself, and also reveals how things have not changed.

This book—the fourth in the Access to Knowledge (A2K) series published by the Access to Knowledge Global Academy (A2KGA)—has its origins both in the A2KGA network and a meeting—the Global Censorship Conference organized at Yale University in 2012. The A2KGA is an informal network of academic and research centres—based in Brazil, China, Egypt, India, South Africa, and the United States of America—committed to research, education, and policy advice promoting access to knowledge, and has previously published books on Access to Knowledge in India, in Brazil, and in Egypt.

Information Society Project
Yale Law School

THE CENTRE FOR internet & society

ITS Instituto de Tecnologia & Sociedade do Rio

THE AMERICAN UNIVERSITY IN CAIRO
SCHOOL OF BUSINESS ACCESS TO KNOWLEDGE FOR DEVELOPMENT A2K4D

unit
UNIVERSITY OF CAPE TOWN
INTELLECTUAL PROPERTY UNIT

Innovation & Technology Policy Lab at Duke UNIVERSITY
Collaboration Across Borders

IIPL 互联网政策与法律研究中心
Institute for the Internet Policy & Law