Introduction to Internet Censorship and Control

Steven J. Murdoch[1] and Hal Roberts[2]

The Internet is and has always been a space where participants battle for control. The two core protocols that define the Internet – TCP and IP – are both designed to allow separate networks to connect to each other easily, so that networks that differ not only in hardware implementation (wired vs. satellite vs. radio networks) but also in their politics of control (consumer vs. research vs. military networks) can interoperate easily. It is a feature of the Internet, not a bug, that China – with its extensive, explicit censorship infrastructure – can interact with the rest of the Internet.

In a collection of articles published as an open access collection at http://cyber.law.harvard.edu/pubrelease/internetcontrol/ and also in a special issue of IEEE Internet Computing[3], we present five peer reviewed papers on the topic of Internet censorship and control. The topics of the papers include a broad look at information controls, censorship of microblogs in China, new modes of online censorship, the balance of power in Internet governance, and control in the certificate authority model.

Initially mechanisms of Internet control were largely developed by members of the Internet community in the form of norms enforced with little or no intervention of courts or law enforcement. Members of the Internet community, especially its technical administrators, enforced these norms by threatening temporary or permanent disconnection from the Internet. For example, the "Usenet Death Penalty[4]" was a punishment which could be imposed on Internet Service Providers (ISPs), preventing their users from posting to Usenet, if the consensus amongst the technical administrators of major ISPs was that the offending ISP was not adequately controlling spam from its customers.

Many hoped that these internally developed and enforced methods of controlling Internet users could be sufficient to preserve the ability for the Internet to function well. By avoiding government interference, the ambition was to achieve freedom of speech and freedom from prejudice. These goals were represented in John Perry Barlow's "Declaration of the Independence of Cyberspace[5]", where he proposed dealing with the conflicts that existed in the Internet at the time though a shared international "Social Contract," rather than by extending national laws to apply to the Internet.

Increasingly however, Internet control mechanisms – including technical, legal, political, and social tools – have been imposed by governments due to a perception that self-regulation is no longer sufficient to deal with challenges increasingly posed by the Internet. Those challenges include the

---

1 Research Fellow, University of Cambridge Computer Laboratory

2 Fellow, Berkman Center for Internet & Society at Harvard University

3 IEEE Internet Computing, Vol. 17, No. 3, May-June 2013.

4 The Jargon File, Eric Raymond (ed.) http://catb.org/jargon/html/U/Usenet-Death-Penalty.html

5 A Declaration of the Independence of Cyberspace, John Perry Barlow. https://projects.eff.org/~barlow/Declaration-Final.html

rapidly growing number and diversity of users, intensifying criminal activity, the role of the Internet as a core social infrastructure, and the diversity of political philosophies of participating countries.

In this collection, M. Christopher Riley's "Anarchy, State, or Utopia? Checks and Balances of Power in Internet Governance" gives an overview of Internet control mechanisms to give context to the discussion of censorship and control in the other articles presented. The article shows how a complex set of checks and balances, spread between governments, companies, international bodies and individuals has evolved over time and is continuously in flux.

Riley describes how the idealistic vision of self-governance of the Internet proved insufficient to deal with more modern challenges, leading to other bodies stepping in to try to deal with the problems faced. Such efforts have not been easy though, as there is not universal agreement on the goals for Internet governance, let alone how to achieve those goals. One particular concern is that this evolution of mechanisms for control will reduce the Internet's power as a force for freedom and turn it into net force for government repression.

There is some reason to believe that this dystopia is possible – enforcement of controls on the Internet can be automated and so are capable of being carried out at far larger scales than controls on other forms of communication. Being able to monitor an entire country's population is a nightmare for civil libertarians and a dream for dictators. Achieving this nightmare / dream for the Internet could be as easy as enabling the right configuration options on existing networking equipment. The aftermath of the Arab Spring revealed how repressive governments used technology to surveil civil society, and how Western companies supplied those governments with surveillance technology, knowing how it would be used.

Encryption and authentication can help resist surveillance, but these technologies are underused. Some of this failing is a result of governments classifying encryption systems as munitions and restricting their distribution. Some of it is a result of the difficulty of correctly using encryption software. As a consequence, people who do use encryption are more likely to stand out in the crowd and so put themselves at risk of more targeted surveillance, which even advanced encryption systems cannot withstand. Again, Western companies have been selling to authoritarian governments software packages that circumvent encryption by exploiting vulnerabilities in commonly used software.

One area where encryption has seen good usage however is HTTPS encrypted web browsing. Initially motivated by the goal of achieving safe Internet commerce, HTTPS has now been applied to encrypt access to webmail services. Webmail over HTTPS does not offer the same level of security as end-to-end email encryption such as OpenPGP. HTTPS only encrypts the communication between the user's web browser and the webmail provider's servers, not the traffic between mail servers. But HTTPS is easier to use than more secure email encryption technologies like OpenPGP. In fact, HTTPS requires no extra software, and most users will not even realise the difference between HTTPS and plain HTTP webmail. And unlike OpenPGP, webmail over HTTPS can be adopted unilaterally by users without them having to persuade all of their communication partners to upgrade too.

The trend for webmail providers allowing HTTPS encrypted access to their services is encouraging because it can help users avoid monitoring by their own governments, at the cost of requiring trust in the webmail provider. However, the mechanisms of control which were put in place to protect HTTPS users are proving increasingly inadequate. Certification Authorities (CAs) are responsible for establishing that the HTTPS site a user is connecting to is in fact run by the owner of the site's domain name. A vulnerability of the CA model is that CAs have the power, through cryptographic credentials

baked into web browser code, to impersonate any website to any user. This power has made CAs targets for attack by criminals, who have successfully obtained fraudulent certificates in a few cases. There has also been fear of governments pressuring CAs into granting fraudulent certificates in order to disguise surveillance operations.

In this collection, these topics are explored in "Trust Darknet: Control and Compromise in the Internet's Certificate Authority Model" by Steven Roosa and Stephen Schultze. The authors have examined a spate of compromises of high-profile Certification Authorities (CAs), and the weaknesses in the CA model which have made such compromises so damaging and hard to manage. Decentralization of CAs has encouraged competition, which has pushed down prices but led to a race to the bottom in terms of security. And, because of technical limitations, the compromise of any CA can lead to the compromise of any website. This situation is far from ideal. The authors examine the legal and economic forces at work and discuss improvements which they hope will reduce the likelihood of CA compromise and the resulting damage of any such compromise.

Measures being considered to protect against these types of attack include forcing CAs to be more transparent about how they grant certificates and how browser vendors include CAs' credentials in web browsers. With these changes, a rogue or compromised CA who issues a certificate to the wrong person can be detected, though perhaps only after the damage has been done. But at least if misbehavior is detected, browsers can blacklist the CA and mitigate future damage. Since being blacklisted by a commonly used browser will destroy the business model of the CA, there is significant incentive for CAs to avoid this fate. It remains to be seen how effective these measures will be, but we can learn from the experience of trying to introduce transparency to another type of control on the Internet – censorship.

Initially censorship on the Internet was widely seen as a futile effort, with Internet pioneer John Gilmore famously saying, "The Net interprets censorship as damage and routes around it.[6]" Governments' first crude attempts at censorship, restricted to the most repressive of countries, were easily defeated. But governments learned from their mistakes, and today's censorship techniques are increasingly effective and widespread – and are used by dictatorships and democracies alike. Techniques for censorship vary, ranging from directly interfering with Internet traffic to pressuring content providers to remove offending material. A variety of motivations for censorship also have appeared, such as political control, child protection, and protection of revenue for copyright holders. Frequently however, a censorship system introduced for one reason may be later used for another; for example the UK system for blocking images of child sexual abuse was used to block The Pirate Bay BitTorrent search engine.

In "Censorship v3.1," Derek E. Bambauer examines how the nature of censorship has changed over time. While this change has been taking place, international bodies have also been fighting for more control over the Internet, seeking to reduce U.S. influence over key Internet decision making bodies. The article then goes on to discuss what can be done to reduce the harm that can come from Internet censorship, including recognising that restricting access to material is censorship (though perhaps defensible censorship), supporting the decentralised nature of Internet governance, and resisting efforts to outsource censorship to companies who are less accountable than governments – so as to get discussion of censorship out in the open.

6 First Nation in Cyberspace, Philip Elmer-Dewitt, TIME International, 6 December 1993, No.49. http://www.chemie.fu-berlin.de/outerspace/internet-article.html

Once it is admitted that censorship is taking place, the debate can move on to topics such as whether the proposed censorship is proportionate, who has jurisdiction when standards vary between countries, and what checks and balances should be put in place. Achieving transparency for Internet censorship has proven challenging, even in mature democracies. Reasons given for not disclosing lists of blocked sites include claims that such lists will increase attention paid to the sites, and that transparency is not required when censorship has been outsourced. Censorship is increasingly outsourced by informally imposing pressure on companies providing Internet access or content, rather than being directly performed by the government.

For these reasons, researchers are increasingly responsible for revealing the extent of censorship. Researchers seek to discover which content is being blocked, by whom and for what reason. While technical studies play an important role here, the results of technical studies are not themselves adequate to give a full picture. Knowing which sites are blocked or which content has been removed is necessary, but we must also understand why sites are blocked. Often sites are blocked even though they fall outside the stated criteria for censorship. Sometimes this over-blocking is an underhanded attempt to avoid criticism, but other times it proves to be a mistake resulting from overzealous interpretations of rules or collateral damage resulting from technical limitations in censorship techniques. Distinguishing these cases is important, because frequent errors make arguments for proportionality of censorship less valid.

In "Not By Technical Means Alone: The Multidisciplinary Challenge of Studying Information Controls," Masashi Crete-Nishihata, Ronald Deibert and Adam Senft describe the mixed-method approach that The OpenNet Initiative took for building a global survey of Internet censorship. This survey combined technical measurements with analysis of political, legal and economic systems behind the information controls. The article discusses the technical and methodological challenges of carrying out the study and illustrates the approach taken through a series of case studies.

The task of casting light on censorship can be particularly challenging when governments deliberately disguise the type of censorship used. For example, governments use laws and intimidation to cause individuals to self-censor rather than directly censoring content. Surveillance, or at least the perception of surveillance, gives its targets a realistic expectation that if they step out of line, they will be at risk. Frequently governments couple surveillance with content removal or blocking so that people are aware of both the government monitoring and the limits of acceptable behavior. The technical measures set the limits and the risk of punishment keeps individuals from testing them. As such, just because something is not blocked doesn't mean that many people will exploit this freedom.

In "Assessing Censorship on Microblogs in China: Discriminatory Keyword Analysis and Impact Evaluation of the 'Real Name Registration' Policy," King-wa Fu, C.H. Chan and Michael Chau examine the topic of self-censorship. Through monitoring the censorship of posts on a popular Chinese microblogging service, they infer which topics are considered sensitive by the censors. From this, they discuss how the use of sensitive terms may have changed when the "Real Name Registration" policy was introduced, increasing accountability of microbloggers and creating a chilling effect amongst people discussing controversial topics.

The articles presented in this collection make it clear that there is no global consensus on what mechanisms of control are best suited for managing conflicts on the Internet, just as there is none for other fields of human endeavour. That said, there is optimism that with vigilance and continuing efforts to maintain transparency the Internet can stay as a force for increasing freedom than a tool for more efficient repression.